EASTHALL PARK

Data Protection Policy

Reviewed and approved by Committee	**2022 Novemeber**
Next review	**2024 October**

This document will be made available in different languages and formats on request, including Braille and audio formats.

DATA PROTECTION POLICY

Introduction

Easthall Park Housing Association Ltd (referred to herein as 'EPHA') is a Data Controller registered with the Information Commissioner's Office (Registration No: Z5655541).

EPHC is committed to ensuring the lawful, fair and transparent management of personal data. This policy sets out how we will do this.

All Directors, Associates, members, employees, volunteers (temporary and permanent) (referred to herein as 'EPHC personnel') have a responsibility to ensure compliance with this policy and associated Appendices which set out EPHC's commitment to process personal data in accordance with the relevant legislation including:

- UK General Data Protection Regulation.
- UK Data Protection Act 2018 (DPA 2018).
- Privacy and Electronic Communications Regulations 2003 (PECR).

Scope

This Policy applies to all personal data held by EPHC that relates to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual including, for example, name, address, email, postcode, CCTV image and photograph and video recordings. Special Category personal data is any information relating to racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual orientation, Trades Union membership and criminal convictions.

This policy applies to personal data held or accessed on EPHC premises and systems or accessed remotely via home or mobile working. Personal data stored on personal and removable devices is also covered by this policy.

Responsibilities for Compliance

The *Board /Committee/Directors* are ultimately responsible for ensuring that EPHC meets its legal obligations.

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

All EPHC personnel, accessing or otherwise processing personal data controlled by EPHC have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection law, this policy and the data protection principles.

The Data Protection Lead/Manager, with advice and assistance from the Data Protection Officer (DPO), RGDP LLP, is responsible for:

- monitoring compliance with this policy and data protection legislation;
- managing personal data breaches and data subject rights requests;
- recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

Compliance

EPHC will comply with its legal obligations and the **data protection principles** by ensuring that personal data is:

- **processed lawfully, fairly and in a transparent manner in relation to individuals**. Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

- **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**. Personal data will only be used for the original purpose it was collected for and these purposes will be made clear to the data subject. If EPHC wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing.

- **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**. EPHC will only collect the minimum personal data required for the purpose. Any personal data deemed to be excessive or no longer required for the purposes collected for will be securely deleted in accordance with EPHC's Retention Policy (Appendix 1). Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

- **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay**. EPHC will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

- **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed**. EPHC will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data will be stated in a Retention Schedule. Data will be disposed of in a responsible manner ensuring confidentiality and security.

- **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**. EPHC will implement appropriate security measures to

protect personal data. Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis. EPHC personnel will keep data secure by taking sensible precautions and following the relevant EPHC policies and procedures relating to data protection.

In addition, EPHC will comply with the 'Accountability Principle' that states that organisations are to be responsible for, and be able to demonstrate, compliance with the above principles.

Data Sharing

In certain circumstances EPHC may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations. In all cases, appropriate security measures will be used when sharing any personal data.

Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose.

Prior to sharing personal data, EPHC will consider any legal implications of doing so.

Data Subjects will be advised of data sharing via the relevant the Privacy Notice.

Data Processors

Where EPHC engages Data Processors to process personal data on its behalf, it will ensure that:

- Data processors have appropriate organisational and technical security measures in place.
- No sub-processors are used without prior written consent from EPHC.
- An appropriate contract or agreement is in place detailing the obligations and requirements placed upon the data processor.

Security Incident & Breach Management

Occasionally EPHC may experience a data security incident or personal data breach; this could be if personal data is:

- Lost: for example, misplacing documents or equipment that contain personal data through human error; via fire, flood or other damage to premises where data is stored.
- Stolen: theft or as a result of a targeted attack on the IT network (cyber-attack).
- Accidently disclosed to an unauthorised individual: for example, email or letter sent to the wrong address.
- Inappropriately accessed or used.

All security incidents or personal data breaches will be reported to and managed by the Data Protection Lead who will be advised and assisted by the DPO.

The Information Commissioner's Office and the individuals affected will be notified promptly, if required.

All security incidents and personal data breaches will be managed in accordance with EPHC's Information Security Incident and Personal Breach Management Procedure (Appendix 2).

To assist with the prevention of personal data breaches, all EPHC personnel must adhere to EPHC's Information Security Policy and procedures (Appendix 3).

Individual Rights

EPHC will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Subject Rights Procedure (Appendix 4). EPHC will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. EPHC will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (sometimes referred to as 'the right to be forgotten') – EPHC will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** – EPHC will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.
- **Right to Object** – by stopping processing personal data, unless legitimate grounds can be demonstrated for the processing which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

Data Protection by Design

EPHC has an obligation to implement technical and organisational measures to demonstrate that data protection has been considered and integrated into its processing activities.

When introducing any new type of processing, particularly using new technologies, it will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and consider the need for a Data Protection Impact Assessment (DPIA) (Appendix 5).

All new policies including the processing of personal data will be reviewed by the Data Protection Lead to ensure compliance with the law and establish if a DPIA is required. Advice and assistance will be provided by the DPO and if it is confirmed that a DPIA is required, it will be carried out in accordance with EPHC's DPIA Procedure.

Training
All EPHC personnel will be made aware of good practice in data protection and where to find guidance and support for data protection issues. Adequate and role specific data protection training will be provided during induction and annually thereafter to everyone who has access to personal data to ensure they understand their responsibilities.

Breach of Policy
Any breaches of this policy may be dealt with in accordance with EPHC's disciplinary procedures.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

Appendices:

1. Retention Procedure and Schedule
2. Information Security Incident and Personal Data Breach Management Procedure
2a Breach reporting form
3. Information Security Policy
4. Data Subject Rights Procedure
5. Data Protection Impact Assessment (DPIA)
6. Privacy Notice(s)
7. Social media use policy
8. Homeworker policy
9. CCTV use policy
10. Model processor/ controller/sharing agreements/due diligence checklist

Dated	31.8.22
Document Owner	Anila Ali DP lead
Approved By	
Review Date	October 2024

Easthall Park Housing Coooperative (EPHC)

Appendix 1 to Data protection policy
Retention Policy and Schedule

Introduction

The UK General Data Protection Regulation (UK GDPR) provides that organisations which process personal data must not retain that data for any longer than is *necessary* for the purposes for which the personal data are processed.

Purpose

This policy details EPHC's approach to the retention, deletion and destruction of personal data. All EPHC personnel are obliged to familiarise themselves with this policy and refer to it on an ongoing basis to ensure that its terms are implemented and complied with.

This procedure applies to all Directors, Associates, members, employees, volunteers (temporary and permanent) (referred to herein as 'EPHC personnel').

Storage of Personal Data

EPHC stores personal data in a variety of ways. This includes hard copy documents, emails, digital documents stored on desktop computers, laptops, phones and other devices, data stored on our servers and in our cloud-based storage, along with data stored by third parties on our behalf.

When updating, rectifying, erasing and deleting any personal data, due care must be taken to ensure that all personal data held in all locations (including back-up storage) and in all forms is dealt with securely and to ensure that a consistent and accurate record of personal data is maintained.

Retention of Personal Data

Different types of personal data may need to be retained for different periods of time depending on the purposes for which the data is processed and the legal and regulatory retention requirements in relation to certain categories of data.

In determining the appropriate retention period consideration should be given to the following factors:

- the purposes for which the personal data is processed;
- the legal basis for processing that personal data;
- legal requirements for retention (particularly employment and health and safety law); and
- regulatory requirements.

An appropriate retention period should be identified for each category of personal data. Data subjects must be informed of the retention period which applies to their personal data or, if there is no fixed retention period, the criteria used to determine that period; and where the purposes for which the data is processed have changed, any new retention period.

All personal data processed by EPHC shall be retained in accordance with the periods set out in the retention schedule below.

Personal data will be retained in accordance with the appropriate retention period and permanently deleted and/or securely destroyed in accordance with this policy. No personal data shall be destroyed or deleted other than in accordance with this policy.

Review and Deletion of Personal Data

A review of the personal data processed by EPHC will be carried out every 2 years. During the course of this review we will:

- Review the retention periods for each category of personal data processed and whether any alteration to these periods is required
- Identify personal data which is due for destruction and deletion
- Arrange for the secure deletion and destruction of personal data which will no longer be retained

Data Subject Rights

Under the GDPR data subjects are entitled, in ***certain circumstances*** to require the erasure of their personal data. Any request from a data subject must be passed to the Data Protection Lead .

A data subject may insist on erasure of their personal data where:

- it is no longer necessary for the purposes for which it was processed;
- where consent has been withdrawn by the data subject;
- where there is no legal basis for the processing of the data; or
- where there is a legal obligation to delete the data.

The data subject's rights to erasure are not absolute and do not apply to personal data where processing is necessary for:

- exercising the rights of freedom of expression;
- to comply with a legal obligation in the public interest or in the exercise of an official authority;
- for public health reasons;
- for archiving purposes; and
- for the establishment, exercise or defence of legal claims.

Where personal data is erased following receipt of a request by a data subject EPHC will confirm in writing to the data subject that their personal data has been destroyed. Such a response shall be issued to the data subject unless it is impossible or requires disproportionate effort to do so.

Where any request for erasure is refused, EPHC will advise the data subject in writing that their request has been refused and detail the reasons for refusal.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review

This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

Date this version September 2022

Data Retention for Easthall Park Housing Co-operative – Housing Files

CURRENT TENANT FILES	RETENTION PERIOD	WHERE DO WE HOLD THIS INFORMATION?	COMMENTS
Application for Housing	6 years after offer accepted	Electronic File	
Tenancy Agreement	Length of Tenancy	Electronic File	
Tenant correspondence to Easthall Park	Length of Tenancy	Electronic File	
Verification of Details	Length of Tenancy	Electronic File	
Share application and obligation of Membership	Length of Tenancy	Electronic File	
Care Plans	Length of Tenancy	Electronic File	
OT Assessments	Length of Tenancy	Electronic File	
Identification	Length of Tenancy	Electronic File	
Records from Police relating to offenders	Length of Tenancy	Electronic File	
Void and Allocation Audit	Length of Tenancy	Electronic File	
Housing Benefit notifications	2 years	Electronic File	
ASB	3 years	Electronic File	Housing Scotland Act 2014 will change this to 3 years
Rent Arrears Letters	2 years	Electronic File	
FORMER TENANT FILES	RETENTION PERIOD		COMMENT
Former Tenant Files remain an operational file until 12 months after EOT date. The file must then be cleared off all documentation with exception of the following:			
Tenancy Agreement	5 years	Electronic File	GDPR will change this to 5 years
Termination Details	5 years	Electronic File	
Rent Arrears	5 years	Electronic File	
ASB	3 years	Electronic File	Housing Scotland Act 2014 will change this to 3 years

Data Retention for Easthall Park Housing Co-operative – HR Files

SUBJECT/RECORD	RETENTION PERIOD	WHERE DO WE HOLD THIS INFORMATION?	COMMENTS/ACCESS
Application for Recruitment - Successful	Period of Employment & 5 Years thereafter	Electronic File & Hard Copy	Senior Management Team
Application forms, interview notes, feedback, panel communications, references	Minimum 6 months to a year from date of interviews. Successful applicants' documents transferred to personal file.	Electronic File & Hard Copy	Director
Redundancy details, calculations of payments, refunds.	6 years from the date of the redundancy	Electronic File	Director & Finance Manager
Documents proving the right to work in the UK	2 years after employment ceases.	Electronic File	Director
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.	Electronic File	Director
Payroll	3 years after the end of the tax year they relate to	Electronic File	Senior Management Team & Payroll Provider
Income tax, NI returns, correspondence with tax office	At least 3 years after the end of the tax year they relate to	Electronic File	Finance Team Payroll Provider Senior Management Team
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place	Electronic File	
Pension records	12 years after the benefit ceases	Electronic File	Senior Management Team
Appraisal Records	To be completed – suggest 2 years after employee contract ends	Electronic File & Hard Copy	Line Manager

Appendix 1 (to Data Protection Policy)

SUBJECT/RECORD	RETENTION PERIOD	WHERE DO WE HOLD THIS INFORMATION?	COMMENTS/ACCESS
Absence Records	To be completed – suggest 2 years after employee contract ends	Electronic File	
Disciplinary records	3 years after the end of the tax year to which they relate	Electronic File & Hard Copy	Chairperson/Director & Senior Management Team
Medical Records	3 years after the end of the tax year to which they relate	Hard Copy	Director
Grievance	3 years after the end of the tax year to which they relate	Electronic File	Director
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate	Electronic File	Senior Management Team
Parental Leave	18 years	Electronic File	Director
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	Electronic File	Director & Senior Management Team
Wages/salary records, expenses, bonuses	6 years	Electronic File & Hard Copy	Director, Finance Manager & Team
Records relating to working time	2 years from the date they were made		
Accident books and records and reports of accidents	3 years after the date of the last entry	Hard Copy Director's Office	
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently – needs to be defined – suggest 7	Health & Safety File Directors Office	
Retirement & Pension Information	7 years after death of data subject		

Miscellaneous Start & Leave Dates	7 Years from end of employment	Electronic File	Director

EASTHALL PARK

Disposal and destruction Policy

Reviewed and approved by Committee	**2022 October**
Next review	**2024 October**

INTRODUCTION

In compliance with data protection law, Easthall Park Housing Cooperative will ensure that any personal data it processes will be protected at all times, retained only as long as is necessary in accordance with Easthall Park Housing Cooperative 's retention Policy and Schedule, and disposed of in the most appropriate manner.

HARD COPY DOCUMENT DESTRUCTION

- Paper documents must be disposed of in a timely manner in accordance with the retention periods specified in Easthall Park Housing Cooperative 's Retention Schedule.

- Documentation that is to be disposed of is to be checked before disposal and any documents that contain personal data or sensitive information must be treated as confidential waste.

- Confidential waste must not be left in areas accessible to the public or in areas where there are people who are not entitled to see it, for example, corridors, open-plan offices, unlocked offices, the reception area or anywhere in view of members of staff/visitors/public who should not have access to that information.

- Any documents containing personal data must be disposed of as follows:

    - *By placing in confidential waste bins or bags*
    - *By shredding*
    - *By burning / incineration*
    - *By secure collection for disposal by specialist contractors, eg, ShredIt*

- Prior to disposal, documents are to be removed from folders, plastic/ paper wallets, box files, poly pockets etc and paper clips, staples and treasury tags are to be removed.

- Recycling bins are available for paper documents that do not contain personal data or other sensitive data which does t require secure disposal or destruction.

ELECTRONIC MEDIA AND DOCUMENT DESTRUCTION

- Electronic documents must be disposed of in a timely manner in accordance the retention periods specified in Easthall Park Housing Cooperative 's Retention Schedule.

- All electronic media devices including PCs, laptops, tablets, hard drives, removable hard drives, data sticks and mobile phones should be returned to the IT Department for destruction / disposal in an appropriate manner when they are no longer required.

- Easthall Park Housing Cooperative uses a specialist company to dispose of electronic equipment. They will provide Easthall Park Housing Cooperative with a Certificate of Secure Data Destruction which specifies the method of destruction. This will include the serial number(s) of any equipment they have disposed of.

- For the disposal and destruction of disks, DVDs, CDs, audio or video tapes (including CCTV footage if applicable), these should be passed to the IT Manager who will record that they have been received and securely destroyed or disposed of.

- For documents, including emails, that are to be permanently deleted, ie, put beyond use, the person deleting the document must do all that is reasonably and practicably possible to ensure that deletion has been done in such a way that the document cannot be recovered. For example, emails should also be deleted from the ‘Deleted Items’ folder.

- If any data subject exercises their right to Correct, Erase or Restrict the processing of any personal data held by Easthall Park Housing Cooperative , we must ensure that this is also corrected on any backup drives or systems, whether they be Easthall Park Housing Cooperative ’s drives/systems or a data processors’.

Any questions relating to this procedure should be addressed to the Governance Manager in the first instance.

Date this version September 2022
Due for Review September 2024

EASTHALL PARK HOUSING COOPERATIVE

Information Security and Personal Data Breach Management Procedure

Introduction

In today's world, information is constantly at risk of being involved in a security incident. Cyberattacks, ransomware, phishing, malware, system and process failure, staff mistakes, lost or stolen devices are examples of how data can be lost or compromised.

EPHC is required to record all incidents that could result in a breach of the data protection regulations. The Data Protection Lead will maintain a register of incidents and whether these have resulted in personal data breaches for EPHC.

A security incident, resulting in a breach could damage EPHC's reputation and our relationship with our stakeholders or expose the organisation, our personnel or customers to the risk of fraud or identity theft. In addition, considerable distress could be caused to the individuals concerned, as a result of which, EPHC could face legal action.

Some breaches must be reported to the Information Commissioners Office within 72 hours of EPHC being made aware. There are also requirements to notify the individuals whose personal data has been involved in the breach, under certain circumstances.

The Information Commissioners Office have the right to impose enforcement notices on EPHC or monetary fines (up to 4% of turnover) for breaches, including the failure to notify a breach.

What is a Security Incident?

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, modification, or destruction of information; interference with information technology operations; or significant violation of our acceptable use policy or information security policy.

Examples of information security incidents

- Computer system intrusion
- Unauthorised access to premises where information is stored
- Unauthorised or inappropriate disclosure of organisation information
- Suspected or actual breaches, compromises, or other unauthorised access to EPHC's systems, data, applications, or accounts
- Unauthorised changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for work) used to store or access EPHC's information.
- An attack that prevents or impairs the authorised use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

A **Security Incident** involving personal data is considered a **Personal Data Breach**. If a security incident does not involve personal data, it will still be logged and investigated under this procedure.

Appendix 2 (to Data Protection Policy)

What is a Personal Data Breach?

A personal data breach is a security incident (as outlined above) leading to the **destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**. It is important to understand that a personal data breach is more than just losing personal data.

Essentially while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

Roles and Responsibilities

All EPHC Personnel

- Reporting any security incidents to the Data Protection Lead
- Assisting with any investigation
- Implementing any actions to contain and recover information

Data Protection Lead / Data Protection Officer

- Recording all security incidents
- Deciding if incident has resulted in a personal data breach
- Manage investigations and actions to contain and recover information
- Notify the relevant staff, ICO, data subjects
- Identify lessons learned and implement actions to reduce future re-occurrence.

Board/Corporate Directors

- Ensure appropriate resources are allocated to assist in breach investigations, containment and recovery
- Review Breach Register and reports

Reporting a Security Incident

It is the responsibility of all personnel to report any suspected or actual Security Incident as soon as possible to the Data Protection Lead at the latest the next working day. It is vital that the Data Protection Lead is notified of the incident promptly in order to ensure EPHC takes all immediate actions available to reduce the impact of the incident, identify if personal data is involved and if notification is required to the Information Commissioners Office (ICO) or any relevant data subjects.

You should report any incident by telephoning the Data Protection Lead , and follow up with an email to foi@easthallpark.org.uk if you are unable to make direct contact via the phone.
The correct form to report on is available from FOI:easthallpark.org.uk

Where an incident involves data or IT systems the Data Protection Lead will notify the IT Support Provider/ IT Co-ordinator as soon as possible.

If an incident is identified out of office hours (over weekends/office closures) this should be reported to info@rgdp.co.uk.

EPHC may also be required to report any security incidents to our regulatory authority(ies).

Containment & Recovery

An Incident requires investigation promptly to contain the situation and also a recovery plan including, where necessary, damage limitation. This will often involve input from across the organisation.

The following will be established:

- Who is required to investigate the breach with the DPO and what resources will be required.

- Who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. *(This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.)*

- Whether there is anything we can do to recover any losses and limit the damage the breach could cause. (*As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that personnel recognise when someone tries to use stolen data to access accounts.)*

- If criminal activity is suspected the Police will be informed.

Assessing the Risks

Some data security incidents will not lead to risks beyond possible inconvenience to those who need the data to do their job. For example, where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the business.

While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the incident. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following will be used to make an assessment:

- What type of data is involved? *If it includes personal data it will be considered a Personal Data Breach.*
- How sensitive is it? *Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)*
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate or the organisation; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about an individual or the organisation? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts

of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff or tenants, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to individuals or the organisation? Are there risks to physical safety or reputation, of financial loss or a combination of these?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification

Notification to ICO

EPHC has to notify the ICO of a personal data breach (via Data Protection Lead via the DPO) where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Incidents have to be assessed on a case by case basis. For example, we will need to notify the ICO about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Appendix A provides examples of what breaches require notification and to whom.

The decision to notify the ICO will be made by Data Protection Lead , with advice from the DPO. A written record of this decision will be recorded in the Breach Register.

Information to be provided to the ICO

The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.

The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.

A description of the likely consequences of the personal data breach.
A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How to notify the ICO

A notifiable breach has to be reported to the ICO within 72 hours of us becoming 'aware' of it. When we become 'aware' of the breach is the point when we know or suspect there has been a personal data breach. We may not discover that a security incident is a personal data breach initially, but as soon as we do know or suspect that personal data is involved then we are 'aware'.

Some examples to help determine when we become aware:

- In the case of a loss of a CD with unencrypted data it is often not possible to ascertain whether unauthorised persons gained access. Nevertheless, such a case has to be notified as there is a reasonable degree of certainty that a breach has occurred; we would become 'aware' when we realised the CD had been lost.
- A third party informs us that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As we have been presented with clear evidence of a breach then there can be no doubt that we have become 'aware'.
- We detect that there has been a possible intrusion into our network. We check our systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, we now have clear evidence of a breach there can be no doubt that we have become 'aware'.

It is recognised that it will often be impossible to investigate a breach fully within the 72 hour time-period and legislation allows for us to provide information to the ICO in phases.

Delayed Notifications

If it is not possible to notify the ICO within 72 hours, when notification is completed it must include the reasons for the delay. We should always aim to notify the ICO as soon as possible even if we do not have much detail at that point.

Notification to Data Subjects

If the breach is sufficiently serious to warrant notification to the public, we must do so without undue delay.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay, unless this would involve disproportionate effort.

If it is not possible to contact the data subjects directly or there is a large volume of data subjects involved, then we should make a public communication or similar measure whereby the data subjects are informed in an equally effective manner. Dedicated messages must be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates or newsletters. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS), prominent website banners, social media posts or notification, postal communications and prominent advertisements in printed media.

Communicating a breach to data subjects allows us to provide information on the risks presented as a result of the breach and the steps the data subjects can take to protect themselves from its potential consequences.

Information to be provided to Data Subjects

We must provide the following information:

- a description of the nature of the breach;
- the name and contact details of the Data Protection Officer or other contact point;
- a description of the likely consequences of the breach; and

- a description of the measures taken or proposed to be taken by us to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- If the data subject wishes to raise a complaint about the breach, this should be escalated to the Data Protection Officer.

Evaluation

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it once completed.

If it was identified that the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable. Also, if the management of the breach was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines of responsibility in the light of experience.

We may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The Data Protection Lead / Data Protection Officer will work with the relevant staff involved in the breach to review process and procedures, to ensure that effective measures have been taken to prevent a recurrence of the breach and to monitor ongoing compliance.

The Data Protection Lead /Data Protection Officer will publicise any identified learning outcomes to all parties who may benefit from the updated guidance or information.

Records Management

A Security Incident and Breach Register will be maintained by the Data Protection Lead and this will be reported to the Board on a regular basis.

A case file will be made for each investigation to ensure a full record of the investigation, any correspondence, and decisions on notifications, are maintained accurately and retained as per the EPHC Records Retention Schedule.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

This document was updated September 2022
It is due for review September 2024.

Appendix A – Notification Guidance
(Taken from Article 29 Working Group adopted guidance)

Examples of personal data breaches and who to notify.
The following non-exhaustive examples will assist in determining whether we need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the ICO	Notify the Data Subject(s)	Notes
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required
Personal data of individuals are infiltrated from a secure website managed by the controller during a cyber-attack.	Yes, report to ICO if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable personal data breach, but still a recordable incident. Appropriate records should be maintained by the controller
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present	Yes, report to the ICO, if there are potential consequences to individuals as this is a loss of availability	Yes, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, the ICO may consider an investigation to assess compliance with the broader security requirements

in the system		other likely consequences	
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them
Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, depending on the type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed	Yes, depending on the type of personal data involved and the severity of possible consequences	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Appendix 2a to the Data Protection policy
Personal Data Breach Reporting Form

To be completed by the person in the organisation who is aware of the circumstances of the breach. It is important to note as much information as you have regarding any breach or suspected breach

What has happened?
Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?
Yes/No

How did you find out about the breach?

When did you discover the breach?
Date:
Time:

When did the breach happen?
Date:
Time:

If **there has been a delay in reporting this breach, please explain why.**

Categories of personal data included in the breach (tick all that apply)

☐Data revealing racial or ethnic origin
☐Political opinions
☐Religious or philosophical beliefs
☐Trade union membership
☐Sex life data
☐Sexual orientation data
☐Gender reassignment data
☐Health data
☐Basic personal identifiers, eg name, contact details
☐Identification data, eg, username, passwords
☐Economic and financial data, eg credit card numbers, bank details
☐Official documents, eg driving licenses, passports

☐Location data eg GPS position
☐Criminal convictions, offences
☐Genetic or biometric (fingerprint or iris recognition) data
☐Not yet known
☐Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

☐Employees
☐Users of technology equipment
☐Subscribers
☐Customers or prospective customers
☐Children
☐Vulnerable adults
☐Not yet known
☐Other (please give details below)

Potential consequences of the breach
Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to the data subjects.

Are the data subjects aware of the breach?
Yes/No
If you answered yes, please specify

Have the staff members involved in this breach received data protection training?
Yes/No

If yes – when?

Cyber incidents only:

Has the confidentiality, integrity and/or availability of our information systems been affected?

Yes/No

If you answered yes, please specify (tick all that apply)

☐Confidentiality
☐Integrity
☐Availability

What is the likely impact on our organisation?

What is the likely recovery time?

Person making this incident notification report

Name:
Job Role:
Email:
Phone:

When completed, please return this form to:

foi@easthallpark.org.uk

Easthall Park Housing Cooperative Ltd

Information Security Procedure

Introduction

Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation. It may include personal information about a living individual, or it may be required for the running of EPHC's business. EPHC is committed to ensuring that all personal data will be processed in accordance with best data security practice and the UK General Data Protection Regulation (UK GDPR).

Purpose

The purpose and objective of this Information Security Policy is to protect EPHC's information assets from all threats, whether internal or external, deliberate or accidental, to protect personal and business information, ensure business continuity and minimise business damage by ensuring that all EPHC personnel understand our requirements for handling personal data and to clarify the standards of data security which we expect to be implemented.

Information will be protected from a loss of:

- Confidentiality: ensuring that information is accessible only to authorised individuals
- Integrity: safeguarding the accuracy and completeness of information and processing methods, and
- Availability: ensuring that authorised users have access to relevant information when required

Responsibility for data security

This policy applies to all EPHC personnel.

All EPHC personnel have a responsibility to apply adequate security to personal data which they handle to prevent it from being unlawfully accessed, lost, wrongfully deleted or damaged and to comply with this policy. The Directors of EPHC are responsible for overseeing this Information Security Policy and, as applicable, developing related policies, procedures and guidelines.

Personal Data

Personal data means information which relates to a living individual who can be identified either from that information alone or when that information is combined with other information.

Security Measures

EPHC is committed to protecting the integrity of the information we hold. A data security breach could have a very serious legal, financial and reputational impact for the business.

Training

Appropriate training will be made available for existing EPHC personnel who have responsibility for handling personal data. Each new employee will be made aware of their obligations for data protection during their induction to the organisation. Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that EPHC personnel are adequately trained.

Compliance

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the organisation's disciplinary policy.

INFORMATION SECURITY PROCEDURES:

All EPHC personnel must adhere to the following procedures to ensure security of EPHC's personal data:

Use of Hardware and systems

Our systems have been designed to enable you to work effectively and securely, and you are expected to use them in a professional manner by:

- Using a strong password which must contain
- Never sharing passwords
- Never sharing devices
- Locking screens and mobile devices when not in use and ensuring they are physically secure
- Ensuring anti-virus is kept up to date
- Not downloading unauthorised software or applications onto any of our hardware
- Not connecting unauthorised devices or equipment (including USB sticks, printers etc…) to our devices or systems
- Not connecting to our systems over unsecured wi-fi

E-Mails

- You should be diligent when using email to ensure that you do not provide unauthorised access to our information, spread viruses or infect our systems with malware.

- Do not click on hyperlinks or open attachments in emails unless you trust the sender

- Encrypt any documents containing special categories of personal data before sending by email

- Double check the recipients before hitting "Send"

Your company email account remains the property of EPHC and we may monitor it from time to time to ensure compliance with this policy.

Printing

Care must be taken when printing including:

- Only print documents for which you absolutely need a hard copy
- Ensure all printing is collected from printers immediately
- Any printing remaining on a printer at the end of the day must be shredded

Storage of hard copy documents

Any hard copy (paper) documents containing personal data must be stored in a locked desk or cupboard with limited access. Any keys for accessing these areas must also be stored securely.

When a document containing personal data is no longer required it should be shredded. ONLY documents that do not contain personal data or sensitive information should be put in general waste or recycling bins.

Protecting Information when travelling

In addition to the measures set out above, particular care must be taken to prevent disclosure of information when out of the office. Avoid situations where others can read your documents (e.g., over your shoulder when on public transport) – if in doubt do not read such documents in public. If you are using a laptop in a public area you must use a privacy screen to reduce the chance of someone being able to read the contents of your screen.

Clear desk

All EPHC personnel are to leave their desk/workstation paper free at the end of the day.

All EPHC personnel are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals.

All office managers should have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

EPHC personnel should make sure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information, if needed to be printed, should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that EPHC personnel securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

All EPHC personnel are to leave their desk/workstation paper free at the end of the day and failure to comply with this instruction, could result in disciplinary action being taken.

Printers and fax machines should be treated with the same care.

Clear screen

All EPHC personnel are expected to log off from their PCs/ laptops when left for long periods and overnight. When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Windows key and 'L'. The company system does this automatically after 15 minutes, however taking this measure will reduce any security risk even further.

Mobile devices through which access to the network can be obtained, for example PDAs, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use. EPHC's personnel should also refer to the company's Bring Your Own Device (BYOD) policy.

EPHC personnel should make sure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Reporting a security breach

If you suspect that a security breach has or may occur you must report it immediately to Data Protection Lead.

What to do if you wish to complain about our approach to data security

If any party involved wishes to complain about our approach to Data Security, they should refer to Data Protection Lead who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.
This version September 2022
Due for review September 2024

Clear Desk and Clear Screen Policy

Clear Desk

All Easthall Park Housing Cooperative personnel are to leave their desk/workstation paper free at the end of the day.

All Easthall Park Housing Cooperative personnel are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives;

All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins;

Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals.

All office managers should have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

Easthall Park Housing Cooperative personnel should make sure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information, if needed to be printed, should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that Easthall Park Housing Cooperative personnel securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

All Easthall Park Housing Cooperative personnel are to leave their desk/workstation paper free at the end of the day and failure to comply with this instruction, could result in disciplinary action being taken.

Printers and fax machines should be treated with the same care.

Clear Screen

All Easthall Park Housing Cooperative personnel are expected to log off from their PCs/ laptops when left for long periods and overnight. When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Windows

key and ‘L’. The company system does this automatically after a given time, however taking this measure will reduce any security risk even further.

Mobile devices through which access to the network can be obtained should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use. Easthall Park Housing Cooperative personnel should also refer to the Bring Your Own Device Policy.

Easthall Park Housing Cooperative personnel should make sure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Care must be taken that screens are not sited such that the information displayed on them can easily been seen by unauthorised persons.

Cameras or other recording devices must not be used in the vicinity of screens which may display sensitive date.

Dated	8.9.22
Document Owner	A Ali
Approved By	Committee
Review Date	October 2024

Easthall Park Housing Cooperative

BRING YOUR OWN DEVICE (BYOD) POLICY

1. PURPOSE OF THIS DOCUMENT

This policy details acceptable use by Users whilst using their own Devices for the processing, which includes but is not not limited to, accessing, viewing, modifying and deleting of data held by our Organisation. It also details acceptable use by Users for accessing our organisation's systems where the User's role requires them to access such data whilst away from their place of work or as otherwise approved by the Organisation.

2. DEFINITIONS

BYOD – Bring Your Own Device	Refers to Users using their own Device or systems (which are not owned or provided by the Organisation) or applications to access and store the Organisation's information, whether at the place of work or remotely, typically connecting to the company's Wireless Service or VPN.
Data Controller	The Data Controller is a person, group or organisation that alone or jointly with others determines the purposes and means of the processing of personal data.
Device	An electronic device recognised as a BYOD, including systems and applications used on such a device.
User	A member of staff, employee, contractor, visitor, volunteer, stakeholder or other person authorised to access and use the Organisation's systems.

3. POLICY INTRODUCTION

This policy covers the use of electronic Devices not owned/issued by the Organisation which could be used to access corporate systems and process data, alongside their own data. Such Devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

If Users wish to use Devices to access organisational systems, data and information, Users may do so provided that they follow the provisions of this policy and the advice and guidance provided through the IT Department.

It is the Organisation's intention to place as few technical and policy restrictions as possible on BYODs, subject to the Organisation meeting its legal obligations, including, but not limited to its legal compliance requirements with regards to data protection law.

The Organisation, as the Data Controller, remains in control of the data regardless of the ownership of the Device. Users are required to keep any information and data belonging to the Organisation securely. This applies to information held on a User's Device, as well as on the Organisation's systems. Users are required to assist and support the Organisation in carrying out its legal and operational obligations, including co-operating with the IT

Department should it be necessary to access or inspect data belonging to the Organisation stored on a Device.

The Organisation reserves the right to refuse, prevent or withdraw access to Users and/or particular Devices or software where it considers that there are unacceptable security or other risks including but not limited to its staff, employees, business, reputation, systems or infrastructure.

4. SYSTEM, DEVICE AND INFORMATION SECURITY

The Organisation takes information and systems security very seriously and invests significant resources to protect data and information in its care. The use of a User's Device must adhere to the organisation's policies with regard to security and compliance with data protection law. In particular, where a User uses a Device as a work tool, Users must maintain the security of the Organisation's data and information which a User processes (which includes, but is not limited to, viewing, accessing, storing or deleting information and data belonging to the Organisation).

From time to time, the Organisation may require that Users install or update approved device management software on their Device.

It is the User's responsibility to familiarise themselves with the Device sufficiently to keep data secure. In practice, this means:

a) preventing the theft and loss of data (using for example Biometric/PIN/Password/Passphrase locks and in accordance with other organisational policies and procedures relating to security and data protection law);
b) keeping information confidential, where appropriate; and
c) maintaining the integrity of data and information.

Users must never retain personal data from the Organisation's systems on their Device. If Users are in any doubt as to whether particular data can be stored on a Device, Users are required to err on the side of caution and consult their manager or seek advice from the IT Department.

Users must at all times:

a) use the Device's security features, such as a Biometric, PIN, Password/Passphrase and automatic lock to help protect the device when not in use.
b) keep the Device software up to date, for example using Windows Update or Software Update services.
c) activate and use encryption services and anti-virus protection if a User's Device features such services.
d) install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the Device has this feature.
e) remove any information and data belonging to the Organisation stored on a User's Device once a User has finished with it, including deleting copies of attachments to emails, such as documents, spreadsheets and data sets.
f) limit the number of emails and other information that Users are syncing to the Device to the minimum required, for example only keep the past 24 hours of email in sync.
g) remove all information and data belonging to the Organisation from the Device and return it to the manufacturers' settings before a User sells, exchanges or disposes of the Device.

h) Upon leaving the Organisation, such as at termination of contract of employment, the Device owner must allow the Device to be audited and all information and data belonging to the Organisation be removed, if requested to do so by the Organisation.

5. LOSS OR THEFT

In the event that a Device is lost or stolen or its security is compromised, Users must promptly report this to the IT Department, in order that they can assist Users to change the password to all organisational services.

It is also recommended that Users also do this for any other services that have accessed via that Device, e.g. social networking sites, online banks, online shops). Users must also cooperate with the IT Department in wiping the device remotely, even if such a wipe results in the loss of User's own data, such as photos, contacts and music.

The Organisation will not monitor the content of User's personal Devices. However the IT Department reserves the right to monitor and log data traffic transferred between a User's Device and Organisational systems, both over internal networks and entering the Organisation via the Internet.

In exceptional circumstances, for instance where the only copy of a document belonging to the Organisation resides on a personal Device, or where the Organisation requires access in order to comply with its legal obligations (e.g. it is obliged to do so by a Court of Law or other law enforcement authority) the Organisation will require access to data and information owned by the Organisation stored on a User's personal Device. Under these circumstances, all reasonable efforts will be made to ensure that the Organisation does not access User's private information.

Users are required to conduct work-related, online activities in line with the Organisations's policies and procedures. This requirement applies equally to BYOD.

6. SUPPORT

The Organisation takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding BYOD Devices, or for any loss or damage resulting from support and advice provided.

7. USE OF PERSONAL CLOUD SERVICES

Personal data as defined by the Data Protection Act 2018 and UK GDPR and confidential information and data belonging to the Organisation may not be stored on personal cloud services (e.g. One Drive / Dropbox etc.)

8. COMPLIANCE AND DISCIPLINARY MATTERS

All Users must comply with this policy, and failure to do so may constitute grounds for action, in accordance with the Organisation's Disciplinary Policy.

9. WHAT TO DO IF YOU WISH TO COMPLAIN ABOUT OUR BRING YOUR OWN DEVICE POLICY?

If any User or potential User wishes to complain about our approach to BYOD they should refer to our Data Protection Lead who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

10. REVIEW CYCLE

Date of this version September 2022
Due for Review September 2024.

Appendix 4 data protection policy

Easthall Park Housing Cooperative

Data Subject Rights Procedures

Introduction

The UK General Data Protection Regulation (UK GDPR) provides all living individuals (data subjects) with certain rights over their personal data. Not all rights are absolute, and some can be subject to exemptions.

This Procedure should be read in conjunction with the Data Protection Policy.

Purpose

The purpose of this procedure is to explain how a data subject can make a rights request in relation to their personal data, as defined in Article 15 to 21 of the GDPR, and how Easthall Park Housing Cooperative will handle requests to ensure compliance with the GDPR and any other relevant legislation.

Where personal data is being processed by Easthall Park Housing Cooperative and the identity of the data subject has been verified, Easthall Park Housing Cooperative will respond to the request and provide the data subject with a response within the obligated timeframe.

Scope

This procedure applies to all Directors, Associates, members, employees (temporary and permanent), volunteers, tenants and other external data subjects (referred to herein as 'Easthall Park Housing Cooperative data subjects').

The following rights involving personal data are covered:

Data Subject Right	GDPR Article
Right of Access (Subject Access Request)	Article 15
Right of Rectification	Article 16
Right of Erasure (Right to be forgotten)	Article 17
Right to restrict processing	Article 18
Right of transfer data (Data Portability)	Article 20
Right to object to processing	Article 21

Responsibilities

All Easthall Park Housing Cooperative personnel, are responsible for adhering to this procedure.

The nominate EPHA data protection officer, RGDP, is responsible for maintaining a register of all rights requests and co-ordinating the collection of personal data and providing any required responses.

Definition of Personal Data

Personal data, for the purposes of this procedure is defined as, any information relating to an identified or identifiable living individual who can be identified, directly or indirectly. Personal data includes facts, opinions or intentions relating to the data subject.

The UK GDPR applies to personal data which is:

- processed wholly or partly by automated means e.g., IT system, CCTV, voicemail forms; or
- intended to form part of a filing system e.g., categorised file that enables personal data to be readily accessible.

Receiving a Valid Request

A data subject can make a request via any method and personnel should always be aware of requests via the following:

Verbal Requests	Email	Fax
Written (letter)	Social Media	Website Contact Forms

A request cannot be progressed if we do not have enough information to clearly locate and identify the personal data within the request. The data subject can be asked for further information in order to help locate the information.

Verifying the Identity of the Data Subject

Where there are any reasonable doubts concerning the identity of the data subject, additional information will be requested to confirm the identity of the data subject.

Once Easthall Park Housing Cooperative is satisfied, a note will be made that this requirement has been met and any copies of identification documents will be shredded (there is no requirement to retain copies of any ID verification). Any originals will be sent back via recorded delivery.

If Easthall Park Housing Cooperative can demonstrate that it is not able to identify the data subject, even after additional information is provided, a refusal notice to act upon the request will be issued.

Requests from parties other than the data subject

There are occasions where a data subject may agree to a third party making a request on their behalf, such as a solicitor or family member.

To protect a data subject's personal data, Easthall Park Housing Cooperative will make all the necessary checks to be satisfied that the individual making the request on behalf of the data subject is entitled to do so. This may include requesting a written authority to make the request (e.g., evidence of consent from the individual) or a more general power of attorney.

No information will be released until Easthall Park Housing Cooperative is satisfied. Easthall Park Housing Cooperative may feel it appropriate to contact an individual directly to discuss the request, for example, if asked to release special category data.

In the event of this, the data subject will be given an overview of the type of information that will be released and the option to:

- view their personal data first and upon consent it will be released to the third party
- grant permission for it to be sent directly to the third party
- withdraw consent and no information will be sent to the third party

Charges

In most cases there will be no fee charged for responding to a request, however where Easthall Park Housing Cooperative can demonstrate that the request is manifestly unfounded or excessive in nature it can either:

- charge a reasonable fee, reflective of the administrative costs of dealing with the request; or
- refuse to act on the request.

A data subject will be informed of such decision, the reason why and how a complaint can be raised with the Information Commissioner's Office (ICO) if they wish to appeal.

If the request relates to access to personal data, where Easthall Park Housing Cooperative has provided one copy of the personal data free of charge, for further copies of the same data, Easthall Park Housing Cooperative shall charge a reasonable fee to the data subject based on administrative costs.

Timescales

Easthall Park Housing Cooperative shall provide a response to the data subject without undue delay and in any event within one month of receipt of a valid request. The day the request is received is day one (for example, if the request is received on 10th August the last day for responding is 10th September). Where there is no corresponding date in the following month the last day of that month will be the last date for responding (e.g., received on 31st August the last day will be 30th September).

This period may be extended by two further months, considering the complexity and number of the requests.

The nominate EPHA data protection officer, RGDP, shall inform the data subject of any extension within one month of receipt of the request, together with the reasons for the delay.

If it is not possible to action the request of the data subject, The nominate EPHA data protection officer, RGDP, shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not progressing and of the possibility of complaining to the ICO.

Responding to Requests

The data in any response shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Where an email or online request for copy data is received, the data shall be provided by email, unless the data subject has requested that it be provided in another form. Any such personal data which is emailed shall be encrypted and subject to appropriate security measures.

Access Requests (Subject Access Requests)

This right enables a data subject to verify that Easthall Park Housing Cooperative is lawfully processing their personal data and to check its accuracy. Where data is being processed by Easthall Park Housing Cooperative and the data subject makes a request to access the data, Easthall Park Housing Cooperative shall provide the data subject with access to the personal data and provide:

- the purpose of the processing;
- the categories of personal data being processed;
- the recipients or categories of recipients to whom we have disclosed or will disclose personal data;
- the retention period for the data (or how we determine that);
- the existence of the right to have us rectify, erase or restrict processing of that data;
- the right to lodge a complaint with the ICO;
- the source of the information if we have not collected the data direct from the subject; and
- the existence of any automated decision making.

Where personal data is transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer.

Easthall Park Housing Cooperative has a duty to ensure other individual's information is treated fairly or protected accordingly. Therefore, before Easthall Park Housing Cooperative releases anything to the data subject or representative it has to

ensure that it's not inappropriately releasing information about another individual who can be identified from that information.

On occasions where somebody else can be identified from that information, Easthall Park Housing Cooperative will not release data relating to the data subject unless the other individual has consented to the release of the information or it is reasonable in all circumstances to release the information without consent.

Easthall Park Housing Cooperative will take the below approach:

- Seek documented consent from other individuals
- Where appropriate redact information so other individuals cannot be identified, such as names / addresses/ identification
- Where appropriate provide a summary of the personal data
- Review whether it would be reasonable to release the information without consent, considering;
- is the information already known by the data subject?
- is the individual acting in their professional capacity and had dealings with the data subject?
- is there a duty of confidentiality owed to the other individual?

The data subject's interests and that of the other individual will be reviewed and considered.

All decisions will be made on a case-by-case basis, taking into consideration other legislation that may force the release of information to the data subject.

The Data Protection Act 2018 makes it an offence to intentionally alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

Rectification Requests

Where the request is for the rectification of inaccurate personal data, Easthall Park Housing Cooperative will restrict further processing of personal data whilst verifying the accuracy.

Where the rectification request is upheld, Easthall Park Housing Cooperative shall inform any third parties who have been sent personal data that the data subject has made a rectification request and instruct all parties what rectification is required.

The exception to notifying third parties is if this proves impossible or involves disproportionate effort.

Erasure Requests

When requested to do so by the data subject, Easthall Park Housing Cooperative will erase personal data without undue delay where the request does not conflict with any legal, regulatory or other such constraints.

This right can only be exercised by data subjects where:

(a) the personal data is no longer necessary in relation to the purpose for which it was collected or processed;
(b) where the data subject's consent to processing is withdrawn;
(c) where the data subject objects to the processing and there are no overriding legitimate grounds for processing;
(d) where there is no legal basis for the processing; or
(e) where there is a legal obligation to delete data.

Where personal data is to be deleted, data held in different locations and in different formats will be reviewed to ensure that all relevant personal data is erased.
Where we have made any personal data public, we shall take reasonable steps (taking into account technology and cost) to notify other controllers processing the data of the data subject's request for erasure.

Easthall Park Housing Cooperative is not required to and will not delete personal data where the processing carried out is necessary for:

(a) exercising the right of freedom of expression;
(b) complying with a legal obligation in the public interest or in the exercise of an official authority;
(c) for public health reasons;
(d) for archiving purposes; or
(e) for the establishment, exercise or defence of legal claims.

Once the relevant personal data has been deleted the data subject shall be advised that the data has been erased unless doing so is impossible or involves disproportionate effort.

Restriction Requests

The data subject shall have the right to restrict (block) processing of their personal data.

This is not an absolute right and the data subject will only be entitled to restriction where:

(a) the accuracy of personal data is contested by the data subject for a period to enable us to verify the accuracy;
(b) the processing is unlawful, and the data subject does not want it to be erased but requests restriction instead;
(c) we no longer need the data for the purpose of the processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims; or

(d) the processing has been objected to and verification of that objection is pending.

Where the data subject exercises their right to restriction, personal data can then only be processed with their consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another person or legal entity or for reasons of important public interest of the UK or an EU Member State.

Where we have restricted any form of processing and that restriction is subsequently to be lifted, we shall advise the data subject accordingly unless doing so is impossible or involves disproportionate effort.

Transfer Requests (Data Portability)

This right allows a data subject to obtain and reuse personal data for their own purposes across different services.

Where a data subject requests a copy of their personal data for the purposes of transferring it from Easthall Park Housing Cooperative to another data controller we shall do so provided:

(a) the legal basis for processing is based on consent or a contract with the data subject; and
(b) the processing is carried out by automated means.

The data subject shall only be provided with the personal data they have provided to Easthall Park Housing Cooperative and the personal data gathered by us in the course of our dealings with the individual or which has been generated from our monitoring of the data subject's activity. This will only be data held electronically.

The data subject is entitled to be provided with their personal data in a structured, commonly used and machine-readable format for transfer to another controller; or where possible to have Easthall Park Housing Cooperative transfer the data direct to another controller.

Objection Requests

A data subject can object to the processing of their personal data, including profiling, on grounds relating to their particular situation. Where a request is received, Easthall Park Housing Cooperative is under an obligation to act upon a request where one of the following conditions applies:

- where their personal data is processed based on the public interest or in the exercise of official authority; or
- where we are processing their personal data based on legitimate interests.

If we can demonstrate that Easthall Park Housing Cooperative has legitimate grounds for the processing which override the interests, rights and freedoms of the

data subject or for the establishment, exercise or defence of legal claims, it is not necessary to cease processing.

This does not apply to direct marketing. Data subjects are entitled to object to direct marketing (in any form) which is sent to them. This is an absolute right and where such a request is received, Easthall Park Housing Cooperative must comply with the request.

Applying Exemptions

The UK Data Protection Act 2018 provides exemptions which enable organisations not to respond to data subject rights in certain circumstances.

Easthall Park Housing Cooperative may be exempt from compliance with the data subject rights if certain exemptions apply. Careful consideration should be given to these exemptions and whether they apply before responding to any request by a data subject. Advice from the Data Protection Officer or legal adviser is recommended. The exemptions for compliance with the request are set out in schedule 2 parts 1, 2 and 3 of the Data Protection Act 2018.

In summary these are:

- **Crime and taxation** – for the prevention or detection of crime; the apprehension or prosecution of offenders or the assessment or collection of tax or duty or an imposition of a similar nature to the extent that those provisions would prejudice the activity.

- **Immigration** – for the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control.

- **Information required to be disclosed by law etc. or in connection with legal proceedings** – to the extent that the application of the provisions would prevent same including disclosure which is necessary for the purpose of or in connection with legal proceedings (including prospective legal proceedings) or for obtaining legal advice or otherwise establishing, exercising or defending legal rights.

- **Functions designed to protect the public** – certain functions carried out to protect the public from financial loss through fraud etc.; to protect charities; for health and safety reasons; to prevent malpractice in a public office; or to protect business interests.

- **Regulatory activity** – relating to certain bodies where the application of the provisions would prejudice the discharge of their function.

- **Legal professional privilege/confidentiality of communications** – some solicitor/client communications or information prepared for the purpose of litigation

- **Self-incrimination** – to the extent that complying would reveal evidence of an offence

- **Corporate finance** – in certain circumstances

- **Management forecasts** - to the extent that the application of the provisions would prejudice the conduct of the business or activity concerned

- **Negotiations** - with the data subject to the extent that the application of the provisions would prejudice those negotiations

- **Confidential references** - given to or provided by Easthall Park Housing Cooperative

- **Health, social work, education and child abuse data** to the extent that the application of the provisions would cause prejudice.

If we apply any exemptions or refuse the request for any reason, we will provide the data subject with the following information:

- the reasons why the request is refused/exemptions applied
- their right to make a complaint to the ICO
- their ability to seek to enforce this right through judicial remedy

Register of Requests

The nominate EPHA data protection officer, RGDP, is responsible for maintaining a register of requests, to allow monitoring of the progress of requests and the volume of requests received.

Records Retention

A copy of all the data retrieved must be taken for reference should the data be challenged by the data subject. These will be maintained in line with the records retention schedule and retained for 1 year.

Complaints / Right to appeal

If the data subject or their representative is not satisfied with the outcome of their rights request, in the first instance, the individual will be encouraged to contact the nominate EPHA data protection officer, RGDP, If they are still not satisfied, they can contact the Information Commissioner's Office directly at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel:
E-mail: casework@ico.org.uk
Website: www.ico.org.uk

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the nominate EPHA data protection officer, RGDP, to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the EPHA data protection lead and/or committee.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

Dated	8.9.22
Document Owner	A Anila
Approved By	Committee
Review Date	June 24

Data Protection Impact Assessment Procedure

Please read this document before completing the DPIA template, contained within the Appendix

Contents

Overview

A Data Protection Impact Assessment ('DPIA') is a tool to help us identify and minimise the data protection risks of new projects. They are part of our accountability obligations under the UK General Data Protection Regulation, and an integral part of the 'data protection by default and by design' approach.

We must do a DPIA for certain types of processing of personal data, or any other processing that is likely to result in a high risk to individuals.

A DPIA must:

1. describe the nature, scope, context and purposes of the processing;
2. assess necessity, proportionality and compliance measures;
3. identify and assess risks to individuals; and
4. identify any additional measures to mitigate those risks.

To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Data Protection Lead will be consulted when completing a DPIA and where appropriate, individuals and relevant experts. Any data processors may also need to assist in completing it.

If we identify a high risk that we cannot mitigate, we must consult the Information Commissioner's Office ('ICO') before starting the processing.

An effective DPIA helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

This procedure explains the principles and process that form the basis of a DPIA. It helps us to understand what a DPIA is for, when we need to carry one out, and how to go about it.

What is a DPIA?

A DPIA is a process designed to help us systematically analyse, identify and minimise the data protection risks of a project or planned change. It is a key part of our accountability obligations under the UK GDPR, and when done properly helps us assess and demonstrate how we comply with all of our data protection obligations.

It does not have to eradicate all risk, but should help us minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

DPIAs are designed to be a flexible and scalable tool that we can apply to a wide range of projects regardless of size. Conducting a DPIA does not have to be complex or time-

consuming in every case, but there must be a level of strictness in proportion to the privacy risks arising.

Why are DPIAs Important?

DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to £10 million or 2% annual turnover.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations. However, DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and Easthall Park Housing Cooperative

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used.

Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information.

In turn, this can create potential benefits for our reputation and relationships with individuals:

- help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations;
- identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on; and
- reduce the ongoing costs of a project by minimising the amount of information we collect where possible and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within Easthall Park Housing Cooperative and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a '**data protection by design'** approach.

How are DPIAs Used?

A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA done by the product developer to inform our own DPIA on our implementation plans.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it's important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point

when there is a realistic opportunity to influence those plans. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of a DPIA back into any project plan. We should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help us manage and review the risks of the processing and the measures put in place on an ongoing basis. We need to keep it under review and reassess if anything changes. In particular, if we make any significant changes to how or why you process personal data, or to the amount of data we collect, we need to show that our DPIA assesses any new risks.

An external change to the wider context of the processing should also prompt us to review our DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing we do or the vulnerability of a particular group of data subjects.

What Kind of 'Risk' do DPIAs Assess?

There is no explicit definition of 'risk' in the UK GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The UK GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

When do we Need to do a DPIA?

We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you **must** do a DPIA if you plan:

Systematic and extensive profiling with significant effects:
"any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".

Large scale use of sensitive data:
"processing on a large scale of special categories of data referred to in Article 9(1) (See Appendix 2) or of personal data relating to criminal convictions and offences referred to in Article 10"

Public monitoring:
"a systematic monitoring of a publicly accessible area on a large scale".

The ICO has also published a list of the kind of processing operations that are likely to be high risk and also **require** a DPIA.

New technologies: processing involving the use of new technologies, or the novel application of existing technologies (including AI). **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
Large-scale profiling: any profiling of individuals on a large scale.
Biometrics: any processing of biometric data.
Genetic data: any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.
Data matching: combining, comparing or matching personal data obtained from multiple sources.
Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
Targeting of children or other vulnerable individuals: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
Risk of physical harm: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

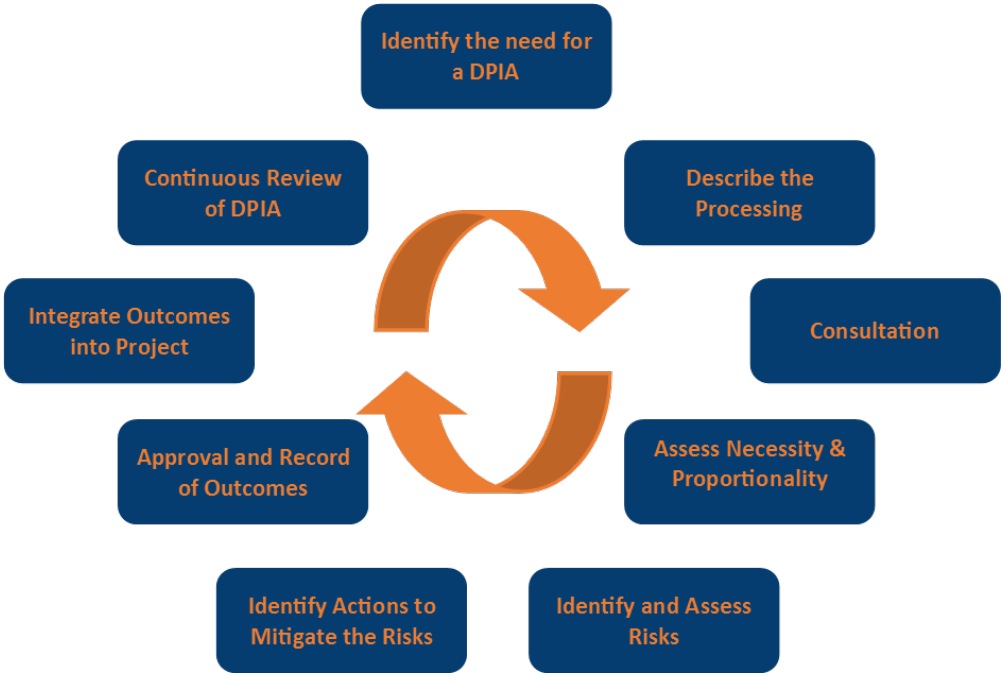
We should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving any use of personal data.

When deciding whether to do a DPIA, we should first answer the screening questions at Appendix 1.

After answering the screening questions, if the decision is made that a DPIA is needed, use the following guidance, as you go along, to complete the DPIA template at Appendix 3.

How to complete a DPIA

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



Responsibility for completing a DPIA

The project manager / lead would usually be best placed to conduct the required DPIA along with any other stakeholders who are able to input into the process.

The Data Protection Lead/DPO will have a significant role in supporting the process, providing advice and guidance, will approve any completed assessment and where required liaise with the Information Commissioners Office.

Step 1: Identify the need for a DPIA

1.1 Contact the Data Protection Lead /DPO and advise them of the new project/change.

1.2 Complete the DPIA Initial Screening Form (Appendix 1) to determine if you need to complete a DPIA.

1.3 If you decide that you do not need to do a DPIA, you should document the decision and the reasons for it on the DPIA Initial Screening Form (Appendix 1).

1.4 If you need to complete a DPIA you should use the DPIA Template (Appendix 3) and complete Step 1, where you should list the types of processing identified from the screening form, the aims of the project and why the need to complete a DPIA was identified.

Jump to Step 1 of the template

Step 2: Describe the Processing

2a Describe how and why you plan to use the personal data

The description must include “the nature, scope, context and purposes of the processing”. The nature of the processing is what you plan to do with the personal data.

This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether there are any data processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

2b The scope of the processing is what the processing covers.

This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

2c The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact.

This might include, for example:

- the source of the data;
- the nature of the relationship with the individuals (tenants, staff);
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern.

2d The purpose of the processing is the reason why you want to process the personal data.

This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole

Jump to Step 2 of the template

Step 3: Consultation

You should always seek the views of individuals (or their representatives) unless there is a good reason not to.

In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of the DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

Do you need to consult anyone else?

If the project involves a **data processor**, you may need to ask them for information and assistance.

You should consult all relevant internal stakeholders, the **IT Support Provider** if this is a new system or change to an existing system to allow Information Security to be considered.

In some circumstances we might also need to consult the ICO once you have completed your DPIA. (Explained in Step 6)

Jump to Step 3 of the template

Step 4: Assess Necessity and Proportionality

You should consider:

- Do your plans help to achieve your purpose?

- Is there any other reasonable way to achieve the same result?

The Article 29 guidelines also say you should include how you ensure data protection compliance, which are a good measure of necessity and proportionality.

In particular, you should include relevant details of:

- your lawful basis for the processing; (see Appendix 2 - Conditions of Processing)
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals' rights;
- measures to ensure your processors comply; and
- safeguards for any international transfers.

Jump to Step 4 of the template

Step 5: Identify and Assess Risks

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material.

In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). You may wish to discuss these with the IT Provider for electronic data transfers.

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

The below Risk Matrix must be considered when assessing likelihood and severity of harm to the rights and freedoms of the individual.

Severity of harm				
	Serious harm	Low risk	High risk	High risk
	Some harm	Low risk	Medium risk	High risk
	Minimal harm	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Jump to Step 5 of the template

Step 6: Identify Actions to Mitigate the Risks

Against each risk identified, record the source of that risk.

You should then consider options for reducing that risk.

For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.

Record whether the measure would reduce or eliminate the risk.

You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of ‘residual risk’ after taking additional measures; and

- whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.

When to Consult the ICO

If you have identified a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so. The focus is on the 'residual risk' after any mitigating measures have been taken. If the DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

How do we consult the ICO?

The DPO will consult with the ICO on Easthall Park Housing Cooperative 's behalf. This is done by completing the online form.

The submission must include:

- a description of the respective roles and responsibilities of any joint controllers or processors;
- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- a copy of the DPIA;

We will be notified if the DPIA has been accepted for consultation within ten days of sending it. If the ICO agree that a DPIA was required, they will review the DPIA.

They will consider whether:

- the processing complies with data protection requirements;
- risks have been properly identified; and
- risks have been reduced to an acceptable level.

The ICO will provide a written response, advising that:

- the risks are acceptable and you can go ahead with the processing;
- you need to take further measures to reduce the risks;
- you have not identified all risks and you need to review your DPIA;
- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed.

In some cases, the ICO may take more formal action. This might include an official warning not to proceed, or imposing a limitation or ban on processing.

If we disagree with the ICO advice we can ask for a review of the decision.

Jump to Step 6 of the template

Step 7: Approval and Record of Outcomes

As part of the approval process, you should submit your assessment to the Named Role/DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.

Jump to Step 7 of the template

Step 8: Integrate Outcomes into Project

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

It is good practice to publish DPIA's to aid transparency and accountability. This could help foster trust in our processing activities, and improve individuals' ability to exercise their rights.

Step 9: Continuous Review of DPIA

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

.

Appendix 1 - DPIA Initial Screening Form

1. Project Details

Project Title / Change Description:	
Project Manager/ Lead details:	
Date of Screening:	

2. Answer yes or no to all the different types of processing listed below

Does the processing you are planning:	**Answer**
Use systematic and extensive profiling or automated decision making to make significant decisions about people?	
Process special category data (see Appendix 2) or criminal offence data on a large scale?	
Systematically monitor a publicly accessible place on a large scale?	
Use new technologies?	
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	
Carry out profiling on a large scale?	
Process biometric or genetic data?	
Combine, compare or match data from multiple sources?	
Process personal data without providing a privacy notice directly to the individual?	
Process personal data in a way which involves tracking individuals' online or offline location or behaviour?	
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	
Process personal data which could result in a risk of physical harm in the event of a security breach?	

3. If the answer is **yes** to any one of these types of processing, then you **must** complete a DPIA. If the answer was **no** to all these types, then you must review the following processing listed below that may require a DPIA

Does the processing involve:	**Answer**
Evaluation or scoring	
Automated decision-making with significant effects	
Systematic monitoring	
Processing of sensitive data or data of a highly personal nature	
Processing on a large scale	
Processing of data concerning vulnerable data subjects.	
Innovative technological or organisational solutions	

Processing involving preventing data subjects from exercising a right or using a service or contract.	

4. If the answer is **yes** to any of these processing types you must discuss the requirement to complete a DPIA with the Data Protection Lead/DPO.

Is DPIA Required?	
Reason for Decision if not completing DPIA:	

If the decision is made that a DPIA is needed, use the above guidance to complete the DPIA template at Appendix 3.

Appendix 2 – Conditions for Processing

Below are the different legal bases available for processing personal data and special categories of data.

Legal Bases for Processing Personal Data:

- 6(1)(a) – Consent of the data subject *(only use consent if there is no other condition that can be used)*
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Categories of Special Category Data:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life and sexual orientation
- Genetic data
- Biometric data used to identify an individual

Conditions for Processing Special Categories of Data:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-pro fit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in

connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 3 -DPIA Template

Data Protection Impact Assessment

For guidance on how to complete this form, it is important to read the above DPIA Procedures before and during completion of this assessment.

This assessment must be commenced at the beginning of any project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes must be integrated back into the project plan.

Name of Organisation	
Project Title / Change Description:	
Project Manager/ Lead details:	
Name of Data Protection Officer	
Date of Assessment:	

Step 1: Identify the need for a DPIA
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project scoping. Summarise why you identified the need for a DPIA. (See DPIA Procedure Step 1 for further guidance).

Step 2: Describe the Processing
2a Describe the nature of the processing: (See DPIA Procedure Step 2 for further guidance)
How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone?

What types of processing identified as likely high risk are involved?
Insert flow diagram showing data flows (optional)

2b Describe the scope of the processing:
(See DPIA Procedure Step 2 for further guidance)

Details of personal data

Please indicate what personal data will be collected/stored/processed, please indicate with an X where applicable.

Administration data

Name	☐
Date of Birth/Age	☐
Gender	☐
Contact details	☐
Unique identifier e.g. student number/NI No.	☐
Other data (please specify):	

Special Categories of data

Racial or ethnic origin	☐
Political opinion	☐
Religious or philosophical beliefs	☐
Trade Union membership	☐
Physical or mental health condition	☐
Sexual life and sexual orientation	☐
Genetic data	☐
Biometric data used to identify an individual	☐

Other sensitive information

Financial information/bank account details	☐
Criminal convictions and offences	☐
Other (please specify):	

Under Article 6 of the UK GDPR one of the following conditions needs to apply before the processing of personal data is lawful. Please indicate which condition applies: (See Appendix 2)

- The individual who the personal data is about has given/will give unambiguous consented to the processing ☐
- The processing is necessary for the performance of a contract with the individual ☐
- The processing is necessary for a legal obligation ☐
- The processing is necessary for the vital interests of someone (i.e. life or death situation) ☐
- The processing is carried out in the public interest or in the exercise of official authority ☐
- The processing is in the legitimate interests of the business or another party and does not prejudice the rights and freedoms of the individual (please provide further details): ☐

If processing Special Category Data, please state which of the conditions for processing specified in Appendix 2 applies.

2c Describe the context of the processing:
(See DPIA Procedure Step 2 for further guidance)

What is the nature of your relationship with the individuals?

How much control will they have?

Would they expect you to use their data in this way?

Do they include children or other vulnerable groups?

Are there prior concerns over this type of processing or security flaws?

Is it novel in any way?

What is the current state of technology in this area?

Are there any current issues of public concern that you should factor in?

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

2d Describe the purposes of the processing:
(See DPIA Procedure Step 2 for further guidance)

What do you want to achieve?

What is the intended effect on individuals?

What are the benefits of the processing for you, and more broadly?

Step 3: Consultation

Consider how to consult with relevant stakeholders: (See DPIA Procedure Step 3 for further guidance)

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Who else do you need to involve within your organisation?

Do you need to ask any relevant data processors to assist?

Do you plan to consult information security experts, or any other experts?

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular:
(See DPIA Procedure Step 4 for further guidance)

What is your lawful basis for processing?

Does the processing actually achieve your purpose?

Is there another way to achieve the same outcome?

How will you prevent function creep?

How will you ensure data quality and data minimisation?

What information will you give individuals?

How will you help to support their rights?

What measures do you take to ensure data processors comply?

How do you safeguard any international transfers?

Step 5: Identify and Assess Risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. (See DPIA Procedure Step 5 for further guidance and Risk Matrix)	Likelihood of Harm	Severity of Harm	Overall risk
Risk No. 01			
Risk No. 02			

Step 6: Identify Actions to Mitigate the Risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5
(See DPIA Procedure Step 6 for further guidance)

Risk	**Actions to reduce or eliminate risk**	**Effect on Risk** *(reduced / eliminated*	**Residual Risk** *(Low/ Medium/ High)*	**Action Approved** *(Yes/No)*

		/ Accepted)		
Risk No. 01				
Risk No. 02				

Step 7: Approval and Record of outcomes

(See DPIA Procedure Step 7 for further guidance)

Item	Signed / Date	Notes
Risk Actions approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
This DPIA will be kept under review by:		*The Data Protection Lead should also review ongoing compliance with DPIA*

Data Protection Impact Assessment

Screening Procedure

This procedure is to be used when a new project, or a change to a project, which involves any processing of personal data is being planned. This can include, but is not exclusive to, new IT systems, marketing campaigns, sharing personal data with other website providers, initiatives involving uses of personal data in new ways.

What is a DPIA?
Data Protection Impact Assessments (DPIA) are a tool to help us identify and minimise the data protection risks of new projects. They are part of our accountability obligations under the General Data Protection Regulation, and an integral part of the 'data protection by default and by design' approach.

An effective DPIA helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

Why are DPIAs important?
Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk to the rights and freedoms of the people whose personal data is being processed (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to €10 million or 2% annual turnover.

How are DPIAs used?
A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA completed by the product developer to inform our own DPIA on our implementation plans.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it is important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point when there is a realistic opportunity to influence those plans.

What kind of 'risk' do DPIA's assess?
There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

When do we need to do a DPIA?
We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk, we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

When deciding whether to do a DPIA, we should first answer the screening questions at Appendix 1.

After answering the screening questions:-

1) if the decision is made that a DPIA is needed, contact the Data Protection Manager or DPO for guidance

or

2) if the decision is made that you do not need to carry out a full DPIA, you should complete the mini DPIA at Appendix 3 and this form should be saved in the main Project File and a copy sent to the Data Protection Manager and DPO.

Appendix 1 - DPIA Initial Screening Form

1. Project Details

Project Title / Change Description:	
Project Manager/ Lead details:	
Date of Screening:	

2. Answer yes or no to all the different types of processing listed below

Does the processing you are planning:	**Answer**
Use systematic and extensive profiling or automated decision making to make significant decisions about people? Includes: Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination Excludes: Processing with little or no effect on people	
Process special category data or criminal offence data on a large scale*? Includes: • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data	

• Trade Union membership data • Genetic data • Biometric data for the purpose of uniquely identifying a person • Health data • Sex life or sexual orientation data • Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data • Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive (*see Appendix 2)	
Systematically monitor a publicly accessible place on a large scale?* Includes processing used to observe, monitor or control people. (*see Appendix 2)	
Use new technologies? The work involves *significant innovation* or use of a *new technology.* Examples could include combining use of fingerprint and face recognition for improved physical access control; new "Internet of Things" applications.	
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	
Carry out profiling on a large scale?* (*see Appendix 2)	
Process biometric or genetic data?	
Combine, compare or match data from multiple sources?	
Process personal data without providing a privacy notice directly to the individual?	
Process personal data in a way which involves tracking individuals' online or offline location or behaviour?	
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	
Process personal data which could result in a risk of physical harm in the event of a security breach?	

3. If the answer is **yes to any one** of these types of processing, then you **must** complete a DPIA. If the answer was **no** to all these types, then you must review the following processing listed below that may require a DPIA

Does the processing involve:	**Answer**

Evaluation or scoring	
Automated decision-making with significant effects	
Systematic monitoring	
Processing of sensitive data or data of a highly personal nature	
Processing on a large scale	
Processing of data concerning vulnerable data subjects.	
Innovative technological or organisational solutions	
Processing involving preventing data subjects from exercising a right or using a service or contract.	

4. If the answer is **yes** to any of these processing types you must discuss the requirement to complete a full DPIA with the Data Protection Manager or DPO.

Is DPIA Required?	**Yes/No**
Reason for Decision if not completing DPIA: If you decide a full DPIA, is **not** required, you should now complete the Mini-DPIA at Appendix 3.	

Appendix 2

Definition of Special Category data:

Personal data relating to:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life and sexual orientation
- Genetic data
- Biometric data used to identify an individual

Definition of 'large scale':

The GDPR does not define what constitutes large-scale, however, the European Data Protection Board Article 29 Working Party, recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity

- The geographical extent of the processing activity

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

Appendix 3

This form is to be used when you have considered the pre-screening questions in the Data Protection Impact Assessment (DPIA) procedure and decided that a full DPIA is **not** necessary. This includes where limited personal (not including special category) data is to be used for a new project/system or for replacement of a supplier of an existing system/service.

If you have not yet considered the pre-screening questions, you must do so before completing this form.

This form should be stored with the DPIA pre-screening form.

Mini-DPIA
Have you considered all the following Data Protection Principles:
Lawfulness, fairness and transparency
• What is the lawful basis you are relying on for the processing?
• Is this fair to the people whose data you are processing?
• Will the people whose personal data you are using expect their details to be used in this way (is this covered in your current relevant Privacy Notice)?
Purpose limitation
• What is the purpose of your proposal and why is it necessary to use personal data to achieve that purpose?
Data minimisation
• What is the minimum personal data necessary to achieve your purpose?
Accuracy
• How will you ensure the personal data is kept accurate and up to date?
Storage limitation
• Has a retention period been established for the personal data and can the system facilitate this (eg, deletion/anonymisation)?
Integrity and confidentiality (security)
• What technology is to be used?

• What are the security arrangements for the personal data?
• Where will the personal data being processed by the supplier be stored geographically?
• If the personal data is to be transferred/stored outside the UK/EEA, what additional arrangements are in place?
• Are there procedures for your employees to follow in relation to how to handle the personal data?
• Is any additional training required for your employees?
Accountability (including data subject rights)
• Have we included a data processor agreement in the contract with the system supplier?
• Is there functionality within the system to extract an individual's personal data in response to a subject rights request?

Risk assessment (to be completed by Data Protection Team in conjunction with project sponsor)

Likelihood of Harm				
	PROBABLE	**GREEN**	**RED**	**RED**
	POSSIBLE	**GREEN**	**AMBER**	**RED**
	REMOTE	**GREEN**	**GREEN**	**GREEN**
		MINIMAL	**SIGNIFICANT**	**SEVERE**
	Severity of Harm			

What does 'harm' mean?

It is something that has an impact on an individual and can affect their circumstances, behaviour, or choices.

For example, a significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

1 Risk to the individual whose data is being processed (e.g. privacy rights, identity theft, etc.)

Describe the source of the risk and nature of the potential impact to the individual(s).	What are you (or will you be) doing to ensure privacy and confidentiality rights are followed as much as possible?
Likelihood of harm to individuals (delete as appropriate):	Remote / Possible but unlikely / Probable (reasonable chance this will happen)
Severity of harm (delete as appropriate):	Minimal / Significant / Severe
Residual risk (delete as appropriate):	GREEN – AMBER – RED

2 Risk to the protection of the data (Security)

Describe the source of the risk and nature of the potential impact to the individual(s).	What are you (or will you be) doing to secure the data as much as possible?
Likelihood of harm to individuals (delete as appropriate):	Remote / Possible but unlikely / Probable (reasonable chance this will happen)
Severity of harm (delete as appropriate):	Minimal / Significant / Severe
Residual risk (delete as appropriate):	GREEN – AMBER – RED

DPO advice

DPO		Date:

Summary of DPO advice:

Review

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Sign off

Each data controller must keep a copy signed off by the Senior Manager responsible for the proposal, or equivalent, as evidence of due diligence.

Senior Manager	Add name and signature (electronic signature is acceptable)	Date:

EASTHALL PARK HOUSING COOPERATIVE - Employee Privacy Notice

EASTHALL PARK HOUSING COOPERATIVE as an employer is a data controller and collects and processes personal data and special category personal data relating its employees to manage the employment relationship it has with you as an employee and after you cease being an employee. We want to be transparent about how we collect and use your data and to meet our data protection obligations.

What personal information we collect and why is it processed?

We collect and process a range of information containing personal data about you. The table below details the personal data collected, the purpose for this and the legal basis for processing:

Personal Information	Purpose	Our legal basis
Basic personal information and contact details including: • Name • Address • date of birth • telephone number • emergency contact details	To maintain accurate employee records and contact details. To be able to contact someone in the event of an emergency. To allow contract, HR and business administration and defence against potential legal claims.	Necessary for the performance of a **contract** with you. Necessary for compliance with a **legal obligation**. Necessary for our **legitimate interests**
Recruitment records including: • CVs, interview notes and assessments • proof of right to work in UK (such as passports and visas) • evidence of education and qualifications • References • Employment Contract • Induction records	To make a decision about your suitability for the role you applied for. To comply with legislative and regulatory requirements To allow contract, HR and business administration and defence against potential legal claims.	Necessary for the performance of a **contract** with you Necessary for compliance with a **legal obligation**. Necessary for our **legitimate interests**
Payroll Information including: • pay and benefits entitlements • bank details • national insurance number	To pay employees and make appropriate tax payments and keep appropriate records. To allow HR and payroll and benefit administration and defence against potential legal claims.	Necessary for the performance of a **contract** with you Necessary for compliance with a l**egal obligation**

Work schedule and Leave including: • days of work • working hours • attendance • leave taken • leave requests • leave authorisation	To pay employees correctly To comply with legal requirements regarding working time To allow resource planning To manage statutory and non-statutory holiday and leave.	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation**. Necessary for our **legitimate interests**
Pension records including: • name • marital status • address • DOB • Salary • Pension age • Beneficiaries	To make appropriate pension payments. To comply with Legislative and regulatory requirements To allow pension administration and defence against potential legal claims. To allow auditing and reporting of Pension schemes	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Performance records including: • appraisal documents • probation and performance reviews • performance improvement plans • records of capability meetings and related correspondence/ warnings	To maintain a record of the operation of performance improvement processes. To allow HR administration and defence against potential legal claims.	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Disciplinary and grievance records including: • records of investigations • witness statements • notes of disciplinary or grievance meetings • correspondence with employees • relevant warnings	To maintain a record of the operation of disciplinary and grievance procedures and their outcome. To allow HR administration and defence against potential legal claims.	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Absence records including: • details of absence taken • reasons for absences • records of absence management discussions	To maintain records of the implementation of absence procedures To ensure that employees receive statutory and	Necessary for the performance of a **contract**

such as Return to Work Interviews • correspondence with employees	contractual sick pay or other pay entitlements and benefits To meet health and safety obligations and comply with the requirement to make reasonable adjustments To allow HR administration and defence against potential legal claims.	Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
CCTV Images	To maintain security of EASTHALL PARK HOUSING COOPERATIVE premises To provide a safe working environment for employees To comply with legislative and regulatory requirements	Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Information about Employee use of business equipment including: • access to computers • desk telephones • mobile phones • software and applications • Internet usage • Emails • Social media	To maintain the operation, security and integrity of business communications systems To provide IT and communications systems support To preventing excessive personal use	Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Photos and Videos	To promote the business of EASTHALL PARK HOUSING COOPERATIVE	Necessary for our **legitimate interests**

Special category personal information	**Purpose for processing**	**Our legal basis for processing**	**Special category legal basis**
Family leave including maternity, paternity, adoption and shared parental leave, parental leave and time off for dependents (which could include information about	To maintain a record of leave To ensure that employees receive statutory and contractual pay entitlements	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation**	Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the

Employee health and sexual orientation).		Necessary for our **legitimate interests**	field of employment.
Occupational Health records including: • medical records • health monitoring information • referrals for treatment such as counselling • reports and correspondence with external practitioners or GP's.	To assess suitability for work To meet Health & Safety obligations To comply with the requirements to provide reasonable adjustments	Necessary for compliance with a **legal obligation.** Necessary for our **legitimate interests**	Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment. Necessary for the purposes of preventative medicine or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health care systems.

We will collect this information in a variety of ways including directly from you, and from third parties as outlined below:

- Recruitment Agencies
- Former employers or other referees
- Occupational Health providers

Who we share your information with?

We will share your data as required by law to administer the working relationship that we have with you.

We may share your data with third parties, including third party service providers that process data on our behalf, in connection with payroll; the provision of employee benefits; the provision of occupational health services and IT services.

In relation to our third-party service providers, we have in place a written contract which only permits them to process your data for specified purposes and in accordance with our instructions. All their employees must be subject to a duty of confidentiality. The contract also requires third party service providers to take appropriate security measures in relation to your personal data which are in line with our policies. They are also not allowed to use your personal data for their own purposes.

How we secure your personal data?

We take the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

In addition, we limit the access that individuals have to your personal data to those who have a business need to know.

We have in place procedures to deal with any suspected data security breach and will notify you and the Information Commissioner's Office of a personal data breach when legally required to do so.

How long will we keep your personal data?

It is important that the personal data that we hold about you is accurate and current. Please keep HR advised of any changes to the personal data that is held, particularly contact details for you and your emergency contacts throughout the course of your employment.

We will hold your personal data for the duration of your employment and for as long as is necessary to fulfil the purposes of satisfying any legal, accounting or reporting requirements that we are subject to. The periods for which your data is held after the end of employment are set out in our Retention Policy.

In determining the retention period, we will consider the amount, nature and sensitivity of the personal data and the potential risk of harm from unauthorised use or disclosure; the purpose for which the data is being processed; and whether we can achieve those purposes through other means; and the applicable legal requirements for holding that data.

Your Rights

You have several rights in relation to your personal data. These are listed below. A fee will not generally be charged for exercising any of these rights unless your requests are manifestly excessive.

- The right to access information about the personal data we process about you and to obtain a copy of it;
- The right to require us to change incorrect or incomplete data;
- The right to require us to erase or stop processing your data; and

- The right to object to the processing of your data where we are relying on its legitimate interests as the legal ground for processing;

If you would like to exercise any of these rights, or if you have any concerns about how your personal data is being processed, please contact the FOI@easthallpark.org.uk

If you still believe that we have not complied with your rights, you can complain to the Information Commissioner's Office. Contact details are available at https://ico.org.uk/make-a-complaint/

What if you do not provide personal data?

You have some obligations under your employment contract to provide us with information. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith which you have as an employee. You may also have to provide us with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the information to us may mean that you are unable to exercise these statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable us to enter a contract of employment with you. If you do not provide other information, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Changes to this Privacy Notice

EASTHALL PARK HOUSING COOPERATIVE reserves the right to update this privacy notice at any time and will provide you with a new notice when making any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

Date of this version September 2022

Due for review September 2024

EASTHALL PARK HOUSING COOPERATIVE (Referred to as 'EASTHALL PARK HOUSING COOPERATIVE ') Privacy Notice for Clients

EASTHALL PARK HOUSING COOPERATIVE is a data controller and will collect and process your personal data. We are required to explain to all clients the personal data we collect, the purpose for processing and the legal basis we are relying on. This is an overview of our Privacy Notice, our full Privacy Notice is available on the EASTHALL PARK HOUSING COOPERATIVE website or you can request a copy from our Data Protection lead.

What personal information does EASTHALL PARK HOUSING COOPERATIVE collect and why is it processed?

EASTHALL PARK HOUSING COOPERATIVE collects and processes a range of information containing personal data about you. We process this information in order to be able to provide our services as a full service legal firm under our contract with you, or to comply with our legal obligations.

We are required to process your personal information when we have a contract with you for the provision of legal services and there may be some occasions where processing of special category personal data (such as health or ethnicity) is required. Where we process special category data it is necessary for the establishment, exercise or defence of legal claims

The personal data we collect, and use will only be the minimum necessary for your case. The following table shows the data we collect and process in relation to your legal case.

<table>
<tr><td>Data processed as necessary for the performance of a contract with you:

Contact Details (name, telephone numbers, email, address), for contacting you regarding the case we are dealing with.
Any personal data that is required to provide you with advice. This could be financial information; special category personal data or any other personal data as is required.

Payment details (bank account/ credit/debit card number), for processing payments required</td><td>Data Processed as necessary to meet a legal obligation:

Identification Documents (copies of passports, driving licence (photographic evidence and home address), for verifying your identification and your home address to comply with anti-money laundering obligations with which EASTHALL PARK HOUSING COOPERATIVE must comply.</td></tr>
<tr><td colspan="2">Data processed that is necessary for the legitimate interests of EASTHALL PARK HOUSING COOPERATIVE or a third party:

Contact Details (name and email), for keeping in touch and to send you information about our services, legal updates and information about our events. You will always be given the option to unsubscribe from receiving these emails and if you do not want to receive this information from EASTHALL PARK HOUSING COOPERATIVE then please email foi@easthallpark.org.uk</td></tr>
</table>

Who has access to your data?

Your information may be shared internally within EASTHALL PARK HOUSING COOPERATIVE on a need to know basis as appropriate. We may share your personal data with the following third parties where it is necessary for the legal service we provide to you:

- Other solicitors instructed by another party in any dispute or claim in which you are involved; your GP or expert witness instructed; any representative appointed to act on your behalf and to solicitors instructed to act as local agents on our behalf
- Service providers and their sub-contractors we are using to run our business including EASTHALL PARK HOUSING COOPERATIVE -for Identity checks; IT services providers; confidential waste disposal services and document storage providers; marketing service providers. Where we use these providers, we have appropriate contractual arrangements in place to ensure that these third parties do not use our data for their own purposes, will treat it with confidence and that they keep the data secure
- We will also share your data as required by law with, for example, Government authorities, law enforcement bodies, regulators for compliance with legal requirements.

How does EASTHALL PARK HOUSING COOPERATIVE protect your personal data?

EASTHALL PARK HOUSING COOPERATIVE takes the security of your data seriously. EASTHALL PARK HOUSING COOPERATIVE has policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by authorised persons who have a need to know in order to perform their duties and are under a duty to maintain the confidentiality and security of such information.

If personal data is transferred outwith the EU we will ensure that adequate safeguards are in place, relying on an adequacy agreement or other contractual terms as appropriate.

How long do we keep your personal data?

Once the case is complete and our legal services have ended, we will hold onto the personal data in your file for at least twenty years in line with the long prescriptive period for making legal claims.

Your rights

As a data subject, you have a number of rights in relation to your personal data. These are listed below.

- The right to access information about your personal data EASTHALL PARK HOUSING COOPERATIVE is processing and to obtain a copy of it;
- The right to require EASTHALL PARK HOUSING COOPERATIVE to change incorrect or incomplete data;
- The right to require EASTHALL PARK HOUSING COOPERATIVE to erase or stop processing your data in certain circumstances; and
- The right to object to the processing of your data where EASTHALL PARK HOUSING COOPERATIVE is relying on its legitimate interests as the legal ground for processing.

A fee will not generally be charged for exercising any of these rights unless your requests are unfounded or are manifestly excessive.

If you would like to exercise any of these rights, or if you have any concerns about how your personal data is being processed, please contact our Data Protection Lead at EASTHALL PARK HOUSING COOPERATIVE at foi@easthallpark.org.uk; or our Data Protection Officer at: info@rgdp.co.uk ; Telephone: 0131 222 3239.

If you still believe that EASTHALL PARK HOUSING COOPERATIVE has not handled your personal data properly or has not complied with your rights, you can complain to the Information Commissioner. Contact details are available at www.ico.org.uk/make-a-complaint/.

We may need to amend this Privacy Notice from time to time and we will notify you of any significant changes that we make.

Date of this version September 2022
Due for review September 2024

Privacy Policy

This website is operated by Easthall Park Housing Co-operative.
We at Easthall Park HC take your privacy seriously and we ask that you read this summary policy statement carefully, as it contains important information on:

- the personal information we collect about you;
- what we do with your personal information; and
- who your personal information might be shared with.

We are the controller of the personal information that we collect from you on our website, which means that we are legally responsible for how we collect, hold and use your personal information. It also means that we are required to comply with data protection laws when collecting, holding and using your personal information.
We have appointed a Data Protection Officer (RGDP) who ensures that we comply with data protection law. If you have any questions about this policy or how we hold or use your personal information, please contact them by e-mail info@rgdp.co.uk or write to: Easthall Park Housing Co-operative, Glenburn Centre, 6 Glenburnie Place, Easthall, Glasgow, G34 9AN.
You can also contact us by: e-mail at FOI@easthallpark.org.uk

Your attention is particularly drawn to section 2 of this policy, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 1 of this policy.
Download a Full Copy of our Data Protection Policy from the website at www.easthallpark.org.uk

1. What personal information do we collect about you and why?

Our website is a place for you to find out more about us, your neighbourhood and the services available to you.
When you visit our website, we collect personal information about you when you:

- report a repair to us;
- make a complaint to us;
- download or submit a housing application form to us;
- complete and submit a “contact us” form to us;

We use such personal information to:

- provide you with the services that you have requested from us;
- communicate with you, including in response to any of your enquiries;
- improve our services and respond to changing needs;

- carry out repairs to your property;
- handle and resolve complaints made by / against you;
- keep the personal information that we hold about you accurate and up-to-date (if you provide any new personal information to us via the website); and

We may not be able to provide the above services to you if you do not provide us with sufficient personal information to allow us to do so.
We may also collect information about you via cookie files. A cookie is a small text file that is placed on to your computer or other access device when you visit our website. We may use cookie files for analytics purposes to gather statistical information on your use of our website.
The information we obtain from our use of cookies will not usually contain your personal information. Although we may obtain information about your computer or other access device, such as your IP address, your browser and / or other internet log information, this will not usually identify you personally.
If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website.

2. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for collecting, holding and using your personal information.
In some circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and sensitive personal information (relating to your health, racial or ethnic origin, religious or other beliefs or sexual orientation) and the personal information and sensitive personal information of other members of your household via our website, you:

- consent to it being used by us as described in section 1 of this policy; and
- confirm that you have informed the other members of your household over the age of 12 years old of the content of this policy and they have provided their consent to their personal information and sensitive personal information being used by us as described in section 1 of this policy.

You and the other members of your household have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 1 of this policy, which you originally agreed to, unless we have another legal reason for doing so.
Other legal reasons for holding and using your personal information are:

- performance and management of the tenancy agreement between us;

- legal and regulatory obligations which apply to us as a Registered Social Landlord or a Property Factor;
- protection of your vital interests; and
- our legitimate interests – while you have a legitimate interest in the protection of your personal information, we also have an overriding legitimate interest in handling and using your personal information, including sharing it with our service providers (listed in section 3 of this policy), for the purposes described in section 1 of this policy.

3. Who do we share your personal information with?

We may share your personal information with the following organisations for the purposes described in section 1 of this policy:

- our contractors to undertake repairs, works and maintenance;
- organisations providing benefits advice and support; and
- Police Scotland and the local authority anti-social behaviour department in relation to complaints involving anti-social or other criminal behaviour.

4. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 1 of this policy, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting us.

5. How do we keep your personal information secure?

The security of your personal information is of paramount importance to us and we use technical and organisational measures to safeguard your personal information.
However, while we will use reasonable efforts to safeguard your personal information, the use of the Internet is not entirely secure and, for this reason, we cannot guarantee the security of any personal information that is transferred by or to you via the Internet. If you have any concerns about the security of your personal information, please contact us for more information.

6. What if you provide us with personal information about somebody else?

We understand that there may be situations where you provide us with personal information about somebody else. In those situations, you confirm that:

- the other individual has consented to you acting for them and to your use of their personal information;

- you have informed the other individual of our identity and the contents of this policy, including the purposes for which we will use that individual's personal information described in section 1 of this policy; and
- the other individual has explicitly consented to our use of that individual's personal information for the purposes described in section 1 of this policy.

This policy will apply to our collection, handling and use of the other individual's personal information in the same manner that it applies to your own personal information.

7. What rights do you have in relation to your personal information that we collect, hold and use?

It is important that the personal information that we collect, hold and use about you is accurate and current. Please keep us informed of any changes by contacting us. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold and use about you.
- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it.
- The transfer of your personal information to another organisation.
- You can also object to us holding and using your personal information where our legal basis is a legitimate interest (either our legitimate interests or those of a third party).

Please contact us if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

8. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to us.
You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The Information Commissioner's website is https://ico.org.uk/ and complaints can be made here. If you would like to receive this policy in alternative format, for example, audio, large print or braille, please contact us.

9. Updates to this policy

We may update this policy at any time, and you should check this policy occasionally to ensure you are aware of the most recent version that will apply each time you access our website.

This version September 2022
Review due September 2024

EASTHALL PARK

Social Media Policy

Reviewed and approved by Committee	**2022 September**
Next review	**2024 September**

Table of Contents

Social Media Policy

1. Introduction

Effective use of social media can bring significant and measurable benefits to Easthall Park Housing Cooperative and its customers. These include opportunities to promote success stories, develop reach within the community and social housing sector, improve customer engagement and attract high quality staff and applicants.

Social media channels can spread Easthall Park Housing Cooperative s' messages quickly and to a range of audiences at little or no cost in order to supplement the Easthall Park Housing Cooperative s channel shift program and, unlike other traditional media channels, they can provide instant feedback from customers.

Along with these benefits come the risks inherent in managing something that is dynamic and unlimited in scale. These include the risk of reputational damage arising from misuse by staff or third parties, threats to the security of sensitive or confidential information, exposure to malware and a negative impact on productivity.

2. Purpose

This Social Media Policy aims to mitigate the risks associated with employees' use of social media. It provides all Easthall Park Housing Cooperative employees with a clear articulation of the expectations around the use of social media.

3. Scope

This policy has been produced for all Easthall Park Housing Cooperative employees including those involved in Easthall Park Housing Cooperative led projects.

4. Equality Analysis

There is potential for social media channels to be used for bullying and harassment of individuals. It is therefore important that the policy is

considered alongside staff conduct guidelines. Employee development will include reference to this policy in induction and management training.

5. Definitions

According to the Chartered Institute of Public Relations (CIPR), social media are: “Internet and mobile-based channels and tools that allow users to interact with each other and share opinions and content. It involves the building of communities or networks and encouraging participation and engagement.” This is the recognised definition for the purpose of this document.

This policy refers to three different types of social media account:-

- Professional Easthall Park Housing Cooperative Housing Account – used by representatives of Easthall Park Housing Cooperative to communicate messages from a departmental or corporate perspective; managed by a Departmental Social Media Champion
- Professional Personal Account – used by an individual member of staff, who is identifiable as an employee of Easthall Park Housing Cooperative through the content of their posts or their profile’s biographical information.
- Private Personal Account – used by an individual primarily for non-work activity.

Social networks covered by this policy include, but are not limited to, Facebook, Twitter, LinkedIn, YouTube, Instagram, Pinterest, Google+ and Tumblr.

6. Legislative Context

- UK GDPR and Data Protection Act 2018 and accompanying guidance in the Information Commissioner's Employment Practices Data Protection Code.
- Human Rights Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699).
- Copyright, Designs and Patents Act 1988

7. Health & Safety Implications

There is potential for social media channels to be used to cause emotional harm or mental distress to others. By producing this policy Easthall Park Housing Cooperative hopes to minimise any distress to its staff caused by the misuse of social media.

8. Policy and Principles

Easthall Park Housing Cooperative employees using social media in a professional capacity, either through a Professional Easthall Park Housing Cooperative account or a Professional Personal Account, should make sure that their communications do not do any of the following:-

- Bring Easthall Park Housing Cooperative into disrepute. For example, by making defamatory comments about individuals, other organisations or groups, or Easthall Park Housing Cooperative ; or posting images that are inappropriate, links to inappropriate content or using inappropriate language.
- Breach confidentiality. For example, revealing confidential information owned by Easthall Park Housing Cooperative relating to its activities, finances, people, or business plans, or the personal data of any individual who has not given informed consent (in writing) for their data to be published.
- Breach copyright. For example, using someone else's image or written content without their permission; failing to give acknowledgement where permission to reproduce something has been obtained
- Do anything that may be considered discriminatory against, or bullying and harassment of, any individual. For example, making offensive or derogatory comments relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive or linking to such content.
- Breach the terms of service of the social network. Each social network has different terms of use and community guidelines, which must be followed.

Employees using social media in a professional capacity should use the same safeguards that they would with any other form of communication about Easthall Park Housing Cooperative in the public sphere. These safeguards may include (but are not limited to):-

- ensuring that the communication has a purpose and benefit to Easthall Park Housing Cooperative
- obtaining a manager's permission before starting a public social media campaign
- checking the appropriateness of the content before it is published
- seeking advice if you are unsure of your objectives or required outcomes.

There should be a clear reason or reasons to set up a Professional Easthall Park Housing Cooperative Account and processes put in place to ensure that it is monitored and updated regularly during business hours.

Effective use of social media can enhance the reputation of Easthall Park Housing Cooperative and inform its customer base of forthcoming events and relevant information. Examples of good practise in the use of social media include but are not limited to:-

- Liking or forwarding a partner organisations post which may be deemed relevant to our customer base
- Providing information on events within Easthall Park Housing Cooperative 's areas of operation
- Providing information on adverse weather, outages, road closures etc within Easthall Park Housing Cooperative 's areas of operation
- Updating customer base on office closures for public holidays, training etc
- Raising awareness of services being offered by Easthall Park Housing Cooperative and projects Easthall Park Housing Cooperative is undertaking.

If you are in any doubt as to whether any form of content is relevant for Easthall Park Housing Cooperative 's corporate social media please consult with your manager.

A corporate services based social media champion will be responsible for:-

- ensuring that the account meets brand guidelines
- making sure that the login details are shared only with those who have a real need to use the account
- revoking access to the account where necessary, such as if an employee leaves the organisation
- ensuring that all content produced for the account is in line with this policy
- ensuring that the account is used regularly
- reporting any incidents where the administrator feels that an employee has misused the social media account.

Employees managing a Easthall Park Housing Cooperative account are expected to remove any comments that fit into the categories outlined under professional use of social media. Additionally, users should also remove comments that are:-

- spam, or trying to sell things
- fraudulent, deceptive or misleading
- in violation of any law or regulation.

Employees are encouraged to think carefully before removing users' comments, to ensure that users with good intentions do not feel that we are placing an unjustified restriction on their freedom of speech.

Social media users are encouraged to regularly check their accounts for messages and respond to any enquiries that they receive in a timely fashion within normal business hours.

Social media users who receive enquiries/approaches from media sources (newspapers, radio, TV) relating to their work at Easthall Park Housing Cooperative are encouraged to notify the departmental director or chief executive for guidance about how to respond (as they would if they received approaches from the media via any other channel).

9. Personal Use of Social Media

Easthall Park Housing Cooperative recognises that many employees will make use of social media in a personal capacity. Easthall Park Housing Cooperative employees using social media in a personal capacity should make sure that their communications do not do any of the following:-

- Bring Easthall Park Housing Cooperative into disrepute.
- Breach confidentiality.
- Breach copyright.
- Breach the terms of service of the social network
- Do anything that may be considered discriminatory against, or bullying and/or harassment of, any individual.

Misuse as outlined above may be regarded as a disciplinary offence.

Employees who openly disclose that they work for Easthall Park Housing Cooperative should include on their profile a statement or disclaimer explaining that the views expressed are theirs alone and that they do not necessarily reflect the views of Easthall Park Housing Cooperative Housing. However, if the content of a post is inappropriate, a disclaimer would not prevent disciplinary action.

To avoid confusion, Easthall Park Housing Cooperative prohibits the use of its logo(s) on social media when used for non-business reasons.

Employees are encouraged to familiarise themselves with privacy settings for each social media platform and choose a privacy level that they consider to be appropriate.

Employees are permitted to make reasonable and appropriate use of personal social media from Easthall Park Housing Cooperative 's computers or mobile devices, provided that this usage is limited to official rest breaks.

10. Procedures

Where it is found that an employee has misused social media, it may be regarded as a disciplinary offence in accordance with organisational disciplinary procedures. Although not exhaustive there are examples of misuse outlined earlier in this document.

Easthall Park Housing Cooperative reserves the right to monitor employees' internet usage in line with the ICT Acceptable Use Policy and the Communications Policy. In line with this, it may instigate an investigation into an employee's internet usage where there are suspicions that the employee has been using social media excessively for personal use when they should be working, or in a way that is in

breach of the rules set out in these policies. Authorisation to instigate an investigation into an employee's internet use can only be done by either the Director of Finance and Corporate Services or the Chief Executive, following consideration of a valid case for this from the individual's line manager.

Easthall Park Housing Cooperative monitors mentions of its brand name and associated terms in order to identify any risks to reputation and to gather customer feedback. Only content that is available in the public domain is subject to monitoring. Data monitored is processed anonymously for analysis purposes and is not held by Easthall Park Housing Cooperative . Easthall Park Housing Cooperative employees are advised to read the privacy guidance provided in this document.

This version September 2022
Due for review September 2024

Working from home or remotely away from the office - Data Protection considerations

Since the start of the Coronavirus pandemic, many people have been working remotely from home instead of their usual place of work. Even as the effects of the pandemic reduce, it seems clear that working from home will continue as new ways of working are adopted. Whether working from an office or remotely from home, data protection laws need to be complied with.

The following guidelines should be followed in all situations where staff are working from home or away from the office.

PURPOSE OF THIS DOCUMENT

This document sets out acceptable policy for compliance with Data Protection Act 2018 and the UK GDPR for users for accessing, viewing, modifying and deleting Easthall Park Housing Cooperative data (ie, processing personal data) and accessing its systems whilst away from the office, ie, in remote offices or your home.

DEFINITIONS

Data Protection Law means the UK General Data Protection Regulation; the UK Data Protection Act 2018; the EU Directive 2002/58/EC on privacy and electronic communications (PECR) as is applicable in the UK; and any laws replacing, amending or supplementing the same and any other applicable data protection or privacy laws.

Remote equipment / Home Worker refers to users using either company provided or your own device or systems or applications, to access and store company information, at your home or remotely, typically connecting to Easthall Park Housing Cooperative ’s Wireless Service or VPN (whichever is relevant).

Data Controller - The Data Controller is a person, group or organisation that alone or jointly with others determines the purposes and means of the processing of personal data. Easthall Park Housing Cooperative is the Data Controller for its employees’ personal data and [add example of other personal data, eg, tenants] (as applicable).

User – A member of staff, employee, contractor, visitor, or another person authorised to access and use Easthall Park Housing Cooperative ’s systems.

Data Processor – a person, group or organisation that processes personal data on the instructions of a Data Controller set out in a written contract.

POLICY INTRODUCTION

This policy covers the use of electronic devices which could be used to access Easthall Park Housing Cooperative ’s systems and store information, alongside employees’ own personal data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies.

Easthall Park Housing Cooperative , as the Data Controller, remains in control of the data regardless of the ownership of the device, or the location in which the data is processed. As an employee of Easthall Park Housing Cooperative you are required to keep any company information and data securely and comply with Data Protection law. You are required to assist and support Easthall Park Housing Cooperative in carrying out its legal and operational obligations, including co-operating with the IT team should it be necessary to access or inspect company data stored on your personal device or equipment at your home.

Easthall Park Housing Cooperative reserves the right to refuse, prevent or withdraw access or permissions for users to work from their homes and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its employees, business, reputation, systems or infrastructure.

Data Protection, Security and Confidentiality of Materials

You must follow Easthall Park Housing Cooperative 's policies and procedures in relation to working with personal data as if you were still based in the office. However, there are additional risks relating to working remotely. You should keep the following in mind:

a) The data protection principles still apply and need to be adhered to, ie, you should only access personal data that is needed for "specified, explicit and legitimate purposes". You should "limit what you take home to only what is necessary" and keep it there for "no longer than is necessary". You must consider "appropriate security", both at home and in transit. Additionally, if required to, you must be able to provide Easthall Park Housing Cooperative with evidence you are complying with these principles.

b) Never leave a computer with personal data on screen. An unauthorised person reading personal data is a data breach.

c) Never leave your computer 'logged on' when unattended. Think about who may access the device when you are not around – whether deliberate or accidental.

d) Ensure that rooms containing computers and other equipment, are secure when unattended, with windows closed and locked and blinds or curtains closed.

e) If making a phone or online conference call remember that it is confidential and consider who is around who might overhear.

f) Levels of Home Security should be at the same level as at work.

g) You should only work within Easthall Park Housing Cooperative 's approved systems, eg, Microsoft Office 365, Teams etc.

h) Do not hold person identifiable information on electronic devices. If you must download a document to your personal device, ensure it is deleted as soon as possible.

i) If using your own device, check for automatic uploads to Cloud storage systems. For example, if you have subscribed to iCloud or Dropbox, you may inadvertently be uploading Easthall Park Housing Cooperative 's documents to your personal account in these applications. You should disable these uploads whilst you are doing Easthall Park Housing Cooperative work.

j) Any paper taken from the office to work at home must be protected in transit and in your home.

k) Paper files should be 'signed out' from the office and 'signed in' again when returned.

l) Ensure paper is transported safely – in a wallet or case

m) Keep paperwork secure at home and out of sight of members of your family and others.

Loss or Theft

In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to Easthall Park Housing Cooperative 's IT department, in order that they can assist you to change the password to all company services and report this as a data breach if appropriate. (You must also cooperate with the IT Department in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.)

Easthall Park Housing Cooperative will not monitor the content of your personal devices, however the IT Department reserves the right to monitor and log data traffic transferred between your device and company systems.

In exceptional circumstances, for instance where Easthall Park Housing Cooperative requires access in order to comply with its legal obligations (e.g. obliged to do so by a Court of law or other law enforcement authority such as the Information Commissioner) Easthall Park Housing Cooperative will require access to company data and information stored on your personal device. Under these circumstances, all reasonable efforts will be made to ensure that Easthall Park Housing Cooperative does not access your private information.

Approval for Working Remotely

Line Managers will consider requests for home working in consultation with individual members of staff and may wish to confirm such arrangements with their senior manager and a Human Resources manager.

Compliance and Disciplinary Matters

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under Easthall Park Housing Cooperative 's disciplinary policy.

Date of this version September 2022
Due for review September 2024

Easthall Park Housing Coooperative (EPHC)

Appendix 1 to Data protection policy
Retention Policy and Schedule

Introduction

The UK General Data Protection Regulation (UK GDPR) provides that organisations which process personal data must not retain that data for any longer than is *necessary* for the purposes for which the personal data are processed.

Purpose

This policy details EPHC's approach to the retention, deletion and destruction of personal data. All EPHC personnel are obliged to familiarise themselves with this policy and refer to it on an ongoing basis to ensure that its terms are implemented and complied with.

This procedure applies to all Directors, Associates, members, employees, volunteers (temporary and permanent) (referred to herein as 'EPHC personnel').

Storage of Personal Data

EPHC stores personal data in a variety of ways. This includes hard copy documents, emails, digital documents stored on desktop computers, laptops, phones and other devices, data stored on our servers and in our cloud-based storage, along with data stored by third parties on our behalf.

When updating, rectifying, erasing and deleting any personal data, due care must be taken to ensure that all personal data held in all locations (including back-up storage) and in all forms is dealt with securely and to ensure that a consistent and accurate record of personal data is maintained.

Retention of Personal Data

Different types of personal data may need to be retained for different periods of time depending on the purposes for which the data is processed and the legal and regulatory retention requirements in relation to certain categories of data.

In determining the appropriate retention period consideration should be given to the following factors:

- the purposes for which the personal data is processed;
- the legal basis for processing that personal data;
- legal requirements for retention (particularly employment and health and safety law); and
- regulatory requirements.

An appropriate retention period should be identified for each category of personal data. Data subjects must be informed of the retention period which applies to their personal data or, if there is no fixed retention period, the criteria used to determine that period; and where the purposes for which the data is processed have changed, any new retention period.

All personal data processed by EPHC shall be retained in accordance with the periods set out in the retention schedule below.

Personal data will be retained in accordance with the appropriate retention period and permanently deleted and/or securely destroyed in accordance with this policy. No personal data shall be destroyed or deleted other than in accordance with this policy.

Review and Deletion of Personal Data

A review of the personal data processed by EPHC will be carried out every 2 years. During the course of this review we will:

- Review the retention periods for each category of personal data processed and whether any alteration to these periods is required
- Identify personal data which is due for destruction and deletion
- Arrange for the secure deletion and destruction of personal data which will no longer be retained

Data Subject Rights

Under the GDPR data subjects are entitled, in ***certain circumstances*** to require the erasure of their personal data. Any request from a data subject must be passed to the Data Protection Lead .

A data subject may insist on erasure of their personal data where:

- it is no longer necessary for the purposes for which it was processed;
- where consent has been withdrawn by the data subject;
- where there is no legal basis for the processing of the data; or
- where there is a legal obligation to delete the data.

The data subject's rights to erasure are not absolute and do not apply to personal data where processing is necessary for:

- exercising the rights of freedom of expression;
- to comply with a legal obligation in the public interest or in the exercise of an official authority;
- for public health reasons;
- for archiving purposes; and
- for the establishment, exercise or defence of legal claims.

Where personal data is erased following receipt of a request by a data subject EPHC will confirm in writing to the data subject that their personal data has been destroyed. Such a response shall be issued to the data subject unless it is impossible or requires disproportionate effort to do so.

Where any request for erasure is refused, EPHC will advise the data subject in writing that their request has been refused and detail the reasons for refusal.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review

This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

Date this version September 2022

Data Retention for Easthall Park Housing Co-operative – Housing Files

CURRENT TENANT FILES	RETENTION PERIOD	WHERE DO WE HOLD THIS INFORMATION?	COMMENTS
Application for Housing	6 years after offer accepted	Electronic File	
Tenancy Agreement	Length of Tenancy	Electronic File	
Tenant correspondence to Easthall Park	Length of Tenancy	Electronic File	
Verification of Details	Length of Tenancy	Electronic File	
Share application and obligation of Membership	Length of Tenancy	Electronic File	
Care Plans	Length of Tenancy	Electronic File	
OT Assessments	Length of Tenancy	Electronic File	
Identification	Length of Tenancy	Electronic File	
Records from Police relating to offenders	Length of Tenancy	Electronic File	
Void and Allocation Audit	Length of Tenancy	Electronic File	
Housing Benefit notifications	2 years	Electronic File	
ASB	3 years	Electronic File	Housing Scotland Act 2014 will change this to 3 years
Rent Arrears Letters	2 years	Electronic File	
FORMER TENANT FILES	RETENTION PERIOD		COMMENT
Former Tenant Files remain an operational file until 12 months after EOT date. The file must then be cleared off all documentation with exception of the following:			
Tenancy Agreement	5 years	Electronic File	GDPR will change this to 5 years
Termination Details	5 years	Electronic File	
Rent Arrears	5 years	Electronic File	
ASB	3 years	Electronic File	Housing Scotland Act 2014 will change this to 3 years

Data Retention for Easthall Park Housing Co-operative – HR Files

SUBJECT/RECORD	RETENTION PERIOD	WHERE DO WE HOLD THIS INFORMATION?	COMMENTS/ACCESS
Application for Recruitment - Successful	Period of Employment & 5 Years thereafter	Electronic File & Hard Copy	Senior Management Team
Application forms, interview notes, feedback, panel communications, references	Minimum 6 months to a year from date of interviews. Successful applicants' documents transferred to personal file.	Electronic File & Hard Copy	Director
Redundancy details, calculations of payments, refunds.	6 years from the date of the redundancy	Electronic File	Director & Finance Manager
Documents proving the right to work in the UK	2 years after employment ceases.	Electronic File	Director
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.	Electronic File	Director
Payroll	3 years after the end of the tax year they relate to	Electronic File	Senior Management Team & Payroll Provider
Income tax, NI returns, correspondence with tax office	At least 3 years after the end of the tax year they relate to	Electronic File	Finance Team Payroll Provider Senior Management Team
Retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place	Electronic File	
Pension records	12 years after the benefit ceases	Electronic File	Senior Management Team
Appraisal Records	To be completed – suggest 2 years after employee contract ends	Electronic File & Hard Copy	Line Manager

Appendix 1 (to Data Protection Policy)

SUBJECT/RECORD	RETENTION PERIOD	WHERE DO WE HOLD THIS INFORMATION?	COMMENTS/ACCESS
Absence Records	To be completed – suggest 2 years after employee contract ends	Electronic File	
Disciplinary records	3 years after the end of the tax year to which they relate	Electronic File & Hard Copy	Chairperson/Director & Senior Management Team
Medical Records	3 years after the end of the tax year to which they relate	Hard Copy	Director
Grievance	3 years after the end of the tax year to which they relate	Electronic File	Director
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate	Electronic File	Senior Management Team
Parental Leave	18 years	Electronic File	Director
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	Electronic File	Director & Senior Management Team
Wages/salary records, expenses, bonuses	6 years	Electronic File & Hard Copy	Director, Finance Manager & Team
Records relating to working time	2 years from the date they were made		
Accident books and records and reports of accidents	3 years after the date of the last entry	Hard Copy Director's Office	
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently – needs to be defined – suggest 7	Health & Safety File Directors Office	
Retirement & Pension Information	7 years after death of data subject		

Miscellaneous Start & Leave Dates	7 Years from end of employment	Electronic File	Director

EASTHALL PARK

Disposal and destruction Policy

Reviewed and approved by Committee	**2022 October**
Next review	**2024 October**

INTRODUCTION

In compliance with data protection law, Easthall Park Housing Cooperative will ensure that any personal data it processes will be protected at all times, retained only as long as is necessary in accordance with Easthall Park Housing Cooperative 's retention Policy and Schedule, and disposed of in the most appropriate manner.

HARD COPY DOCUMENT DESTRUCTION

- Paper documents must be disposed of in a timely manner in accordance with the retention periods specified in Easthall Park Housing Cooperative 's Retention Schedule.

- Documentation that is to be disposed of is to be checked before disposal and any documents that contain personal data or sensitive information must be treated as confidential waste.

- Confidential waste must not be left in areas accessible to the public or in areas where there are people who are not entitled to see it, for example, corridors, open-plan offices, unlocked offices, the reception area or anywhere in view of members of staff/visitors/public who should not have access to that information.

- Any documents containing personal data must be disposed of as follows:

    - *By placing in confidential waste bins or bags*
    - *By shredding*
    - *By burning / incineration*
    - *By secure collection for disposal by specialist contractors, eg, ShredIt*

- Prior to disposal, documents are to be removed from folders, plastic/ paper wallets, box files, poly pockets etc and paper clips, staples and treasury tags are to be removed.

- Recycling bins are available for paper documents that do not contain personal data or other sensitive data which does t require secure disposal or destruction.

ELECTRONIC MEDIA AND DOCUMENT DESTRUCTION

- Electronic documents must be disposed of in a timely manner in accordance the retention periods specified in Easthall Park Housing Cooperative 's Retention Schedule.

- All electronic media devices including PCs, laptops, tablets, hard drives, removable hard drives, data sticks and mobile phones should be returned to the IT Department for destruction / disposal in an appropriate manner when they are no longer required.

- Easthall Park Housing Cooperative uses a specialist company to dispose of electronic equipment. They will provide Easthall Park Housing Cooperative with a Certificate of Secure Data Destruction which specifies the method of destruction. This will include the serial number(s) of any equipment they have disposed of.

- For the disposal and destruction of disks, DVDs, CDs, audio or video tapes (including CCTV footage if applicable), these should be passed to the IT Manager who will record that they have been received and securely destroyed or disposed of.

- For documents, including emails, that are to be permanently deleted, ie, put beyond use, the person deleting the document must do all that is reasonably and practicably possible to ensure that deletion has been done in such a way that the document cannot be recovered. For example, emails should also be deleted from the ‘Deleted Items’ folder.

- If any data subject exercises their right to Correct, Erase or Restrict the processing of any personal data held by Easthall Park Housing Cooperative , we must ensure that this is also corrected on any backup drives or systems, whether they be Easthall Park Housing Cooperative ’s drives/systems or a data processors’.

Any questions relating to this procedure should be addressed to the Governance Manager in the first instance.

Date this version September 2022
Due for Review September 2024

Appendix 2 (to Data Protection Policy)

EASTHALL PARK HOUSING COOPERATIVE

Information Security and Personal Data Breach Management Procedure

Introduction

In today's world, information is constantly at risk of being involved in a security incident. Cyberattacks, ransomware, phishing, malware, system and process failure, staff mistakes, lost or stolen devices are examples of how data can be lost or compromised.

EPHC is required to record all incidents that could result in a breach of the data protection regulations. The Data Protection Lead will maintain a register of incidents and whether these have resulted in personal data breaches for EPHC.

A security incident, resulting in a breach could damage EPHC's reputation and our relationship with our stakeholders or expose the organisation, our personnel or customers to the risk of fraud or identity theft. In addition, considerable distress could be caused to the individuals concerned, as a result of which, EPHC could face legal action.

Some breaches must be reported to the Information Commissioners Office within 72 hours of EPHC being made aware. There are also requirements to notify the individuals whose personal data has been involved in the breach, under certain circumstances.

The Information Commissioners Office have the right to impose enforcement notices on EPHC or monetary fines (up to 4% of turnover) for breaches, including the failure to notify a breach.

What is a Security Incident?

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, modification, or destruction of information; interference with information technology operations; or significant violation of our acceptable use policy or information security policy.

Examples of information security incidents

- Computer system intrusion
- Unauthorised access to premises where information is stored
- Unauthorised or inappropriate disclosure of organisation information
- Suspected or actual breaches, compromises, or other unauthorised access to EPHC's systems, data, applications, or accounts
- Unauthorised changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for work) used to store or access EPHC's information.
- An attack that prevents or impairs the authorised use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

A **Security Incident** involving personal data is considered a **Personal Data Breach**. If a security incident does not involve personal data, it will still be logged and investigated under this procedure.

Appendix 2 (to Data Protection Policy)

What is a Personal Data Breach?

A personal data breach is a security incident (as outlined above) leading to the **destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**. It is important to understand that a personal data breach is more than just losing personal data.

Essentially while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

Roles and Responsibilities

All EPHC Personnel

- Reporting any security incidents to the Data Protection Lead
- Assisting with any investigation
- Implementing any actions to contain and recover information

Data Protection Lead / Data Protection Officer

- Recording all security incidents
- Deciding if incident has resulted in a personal data breach
- Manage investigations and actions to contain and recover information
- Notify the relevant staff, ICO, data subjects
- Identify lessons learned and implement actions to reduce future re-occurrence.

Board/Corporate Directors

- Ensure appropriate resources are allocated to assist in breach investigations, containment and recovery
- Review Breach Register and reports

Reporting a Security Incident

It is the responsibility of all personnel to report any suspected or actual Security Incident as soon as possible to the Data Protection Lead at the latest the next working day. It is vital that the Data Protection Lead is notified of the incident promptly in order to ensure EPHC takes all immediate actions available to reduce the impact of the incident, identify if personal data is involved and if notification is required to the Information Commissioners Office (ICO) or any relevant data subjects.

You should report any incident by telephoning the Data Protection Lead , and follow up with an email to foi@easthallpark.org.uk if you are unable to make direct contact via the phone.
The correct form to report on is available from FOI:easthallpark.org.uk

Where an incident involves data or IT systems the Data Protection Lead will notify the IT Support Provider/ IT Co-ordinator as soon as possible.

If an incident is identified out of office hours (over weekends/office closures) this should be reported to info@rgdp.co.uk.

EPHC may also be required to report any security incidents to our regulatory authority(ies).

Containment & Recovery

An Incident requires investigation promptly to contain the situation and also a recovery plan including, where necessary, damage limitation. This will often involve input from across the organisation.

The following will be established:

- Who is required to investigate the breach with the DPO and what resources will be required.

- Who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. *(This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.)*

- Whether there is anything we can do to recover any losses and limit the damage the breach could cause. (*As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that personnel recognise when someone tries to use stolen data to access accounts.)*

- If criminal activity is suspected the Police will be informed.

Assessing the Risks

Some data security incidents will not lead to risks beyond possible inconvenience to those who need the data to do their job. For example, where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the business.

While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the incident. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following will be used to make an assessment:

- What type of data is involved? *If it includes personal data it will be considered a Personal Data Breach.*
- How sensitive is it? *Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)*
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate or the organisation; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about an individual or the organisation? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts

of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff or tenants, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to individuals or the organisation? Are there risks to physical safety or reputation, of financial loss or a combination of these?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification

Notification to ICO

EPHC has to notify the ICO of a personal data breach (via Data Protection Lead via the DPO) where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Incidents have to be assessed on a case by case basis. For example, we will need to notify the ICO about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Appendix A provides examples of what breaches require notification and to whom.

The decision to notify the ICO will be made by Data Protection Lead , with advice from the DPO. A written record of this decision will be recorded in the Breach Register.

Information to be provided to the ICO

The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.

The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.

A description of the likely consequences of the personal data breach.
A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How to notify the ICO

A notifiable breach has to be reported to the ICO within 72 hours of us becoming 'aware' of it. When we become 'aware' of the breach is the point when we know or suspect there has been a personal data breach. We may not discover that a security incident is a personal data breach initially, but as soon as we do know or suspect that personal data is involved then we are 'aware'.

Some examples to help determine when we become aware:

- In the case of a loss of a CD with unencrypted data it is often not possible to ascertain whether unauthorised persons gained access. Nevertheless, such a case has to be notified as there is a reasonable degree of certainty that a breach has occurred; we would become 'aware' when we realised the CD had been lost.
- A third party informs us that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As we have been presented with clear evidence of a breach then there can be no doubt that we have become 'aware'.
- We detect that there has been a possible intrusion into our network. We check our systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, we now have clear evidence of a breach there can be no doubt that we have become 'aware'.

It is recognised that it will often be impossible to investigate a breach fully within the 72 hour time-period and legislation allows for us to provide information to the ICO in phases.

Delayed Notifications

If it is not possible to notify the ICO within 72 hours, when notification is completed it must include the reasons for the delay. We should always aim to notify the ICO as soon as possible even if we do not have much detail at that point.

Notification to Data Subjects

If the breach is sufficiently serious to warrant notification to the public, we must do so without undue delay.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay, unless this would involve disproportionate effort.

If it is not possible to contact the data subjects directly or there is a large volume of data subjects involved, then we should make a public communication or similar measure whereby the data subjects are informed in an equally effective manner. Dedicated messages must be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates or newsletters. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS), prominent website banners, social media posts or notification, postal communications and prominent advertisements in printed media.

Communicating a breach to data subjects allows us to provide information on the risks presented as a result of the breach and the steps the data subjects can take to protect themselves from its potential consequences.

Information to be provided to Data Subjects

We must provide the following information:

- a description of the nature of the breach;
- the name and contact details of the Data Protection Officer or other contact point;
- a description of the likely consequences of the breach; and

- a description of the measures taken or proposed to be taken by us to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- If the data subject wishes to raise a complaint about the breach, this should be escalated to the Data Protection Officer.

Evaluation

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it once completed.

If it was identified that the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable. Also, if the management of the breach was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines of responsibility in the light of experience.

We may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The Data Protection Lead / Data Protection Officer will work with the relevant staff involved in the breach to review process and procedures, to ensure that effective measures have been taken to prevent a recurrence of the breach and to monitor ongoing compliance.

The Data Protection Lead /Data Protection Officer will publicise any identified learning outcomes to all parties who may benefit from the updated guidance or information.

Records Management

A Security Incident and Breach Register will be maintained by the Data Protection Lead and this will be reported to the Board on a regular basis.

A case file will be made for each investigation to ensure a full record of the investigation, any correspondence, and decisions on notifications, are maintained accurately and retained as per the EPHC Records Retention Schedule.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

This document was updated September 2022
It is due for review September 2024.

Appendix A – Notification Guidance
(Taken from Article 29 Working Group adopted guidance)

Examples of personal data breaches and who to notify.
The following non-exhaustive examples will assist in determining whether we need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the ICO	Notify the Data Subject(s)	Notes
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required
Personal data of individuals are infiltrated from a secure website managed by the controller during a cyber-attack.	Yes, report to ICO if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable personal data breach, but still a recordable incident. Appropriate records should be maintained by the controller
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present	Yes, report to the ICO, if there are potential consequences to individuals as this is a loss of availability	Yes, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, the ICO may consider an investigation to assess compliance with the broader security requirements

in the system		other likely consequences	
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them
Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, depending on the type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed	Yes, depending on the type of personal data involved and the severity of possible consequences	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Appendix 2a to the Data Protection policy
Personal Data Breach Reporting Form

To be completed by the person in the organisation who is aware of the circumstances of the breach. It is important to note as much information as you have regarding any breach or suspected breach

What has happened?
Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?
Yes/No

How did you find out about the breach?

When did you discover the breach?
Date:
Time:

When did the breach happen?
Date:
Time:

If **there has been a delay in reporting this breach, please explain why.**

Categories of personal data included in the breach (tick all that apply)

☐Data revealing racial or ethnic origin
☐Political opinions
☐Religious or philosophical beliefs
☐Trade union membership
☐Sex life data
☐Sexual orientation data
☐Gender reassignment data
☐Health data
☐Basic personal identifiers, eg name, contact details
☐Identification data, eg, username, passwords
☐Economic and financial data, eg credit card numbers, bank details
☐Official documents, eg driving licenses, passports

☐Location data eg GPS position
☐Criminal convictions, offences
☐Genetic or biometric (fingerprint or iris recognition) data
☐Not yet known
☐Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

☐Employees
☐Users of technology equipment
☐Subscribers
☐Customers or prospective customers
☐Children
☐Vulnerable adults
☐Not yet known
☐Other (please give details below)

Potential consequences of the breach
Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to the data subjects.

Are the data subjects aware of the breach?
Yes/No
If you answered yes, please specify

Have the staff members involved in this breach received data protection training?
Yes/No

If yes – when?

Cyber incidents only:

Has the confidentiality, integrity and/or availability of our information systems been affected?

Yes/No

If you answered yes, please specify (tick all that apply)

☐Confidentiality
☐Integrity
☐Availability

What is the likely impact on our organisation?

What is the likely recovery time?

Person making this incident notification report

Name:
Job Role:
Email:
Phone:

When completed, please return this form to:

foi@easthallpark.org.uk

Easthall Park Housing Cooperative Ltd

Information Security Procedure

Introduction

Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation. It may include personal information about a living individual, or it may be required for the running of EPHC's business. EPHC is committed to ensuring that all personal data will be processed in accordance with best data security practice and the UK General Data Protection Regulation (UK GDPR).

Purpose

The purpose and objective of this Information Security Policy is to protect EPHC's information assets from all threats, whether internal or external, deliberate or accidental, to protect personal and business information, ensure business continuity and minimise business damage by ensuring that all EPHC personnel understand our requirements for handling personal data and to clarify the standards of data security which we expect to be implemented.

Information will be protected from a loss of:

- Confidentiality: ensuring that information is accessible only to authorised individuals
- Integrity: safeguarding the accuracy and completeness of information and processing methods, and
- Availability: ensuring that authorised users have access to relevant information when required

Responsibility for data security

This policy applies to all EPHC personnel.

All EPHC personnel have a responsibility to apply adequate security to personal data which they handle to prevent it from being unlawfully accessed, lost, wrongfully deleted or damaged and to comply with this policy. The Directors of EPHC are responsible for overseeing this Information Security Policy and, as applicable, developing related policies, procedures and guidelines.

Personal Data

Personal data means information which relates to a living individual who can be identified either from that information alone or when that information is combined with other information.

Security Measures

EPHC is committed to protecting the integrity of the information we hold. A data security breach could have a very serious legal, financial and reputational impact for the business.

Training

Appropriate training will be made available for existing EPHC personnel who have responsibility for handling personal data. Each new employee will be made aware of their obligations for data protection during their induction to the organisation. Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that EPHC personnel are adequately trained.

Compliance

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the organisation's disciplinary policy.

INFORMATION SECURITY PROCEDURES:

All EPHC personnel must adhere to the following procedures to ensure security of EPHC's personal data:

Use of Hardware and systems

Our systems have been designed to enable you to work effectively and securely, and you are expected to use them in a professional manner by:

- Using a strong password which must contain
- Never sharing passwords
- Never sharing devices
- Locking screens and mobile devices when not in use and ensuring they are physically secure
- Ensuring anti-virus is kept up to date
- Not downloading unauthorised software or applications onto any of our hardware
- Not connecting unauthorised devices or equipment (including USB sticks, printers etc…) to our devices or systems
- Not connecting to our systems over unsecured wi-fi

E-Mails

- You should be diligent when using email to ensure that you do not provide unauthorised access to our information, spread viruses or infect our systems with malware.

- Do not click on hyperlinks or open attachments in emails unless you trust the sender

- Encrypt any documents containing special categories of personal data before sending by email

- Double check the recipients before hitting "Send"

Your company email account remains the property of EPHC and we may monitor it from time to time to ensure compliance with this policy.

Printing

Care must be taken when printing including:

- Only print documents for which you absolutely need a hard copy
- Ensure all printing is collected from printers immediately
- Any printing remaining on a printer at the end of the day must be shredded

Storage of hard copy documents

Any hard copy (paper) documents containing personal data must be stored in a locked desk or cupboard with limited access. Any keys for accessing these areas must also be stored securely.

When a document containing personal data is no longer required it should be shredded. ONLY documents that do not contain personal data or sensitive information should be put in general waste or recycling bins.

Protecting Information when travelling

In addition to the measures set out above, particular care must be taken to prevent disclosure of information when out of the office. Avoid situations where others can read your documents (e.g., over your shoulder when on public transport) – if in doubt do not read such documents in public. If you are using a laptop in a public area you must use a privacy screen to reduce the chance of someone being able to read the contents of your screen.

Clear desk

All EPHC personnel are to leave their desk/workstation paper free at the end of the day.

All EPHC personnel are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals.

All office managers should have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

EPHC personnel should make sure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information, if needed to be printed, should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that EPHC personnel securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

All EPHC personnel are to leave their desk/workstation paper free at the end of the day and failure to comply with this instruction, could result in disciplinary action being taken.

Printers and fax machines should be treated with the same care.

Clear screen

All EPHC personnel are expected to log off from their PCs/ laptops when left for long periods and overnight. When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Windows key and 'L'. The company system does this automatically after 15 minutes, however taking this measure will reduce any security risk even further.

Mobile devices through which access to the network can be obtained, for example PDAs, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use. EPHC's personnel should also refer to the company's Bring Your Own Device (BYOD) policy.

EPHC personnel should make sure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Reporting a security breach

If you suspect that a security breach has or may occur you must report it immediately to Data Protection Lead.

What to do if you wish to complain about our approach to data security

If any party involved wishes to complain about our approach to Data Security, they should refer to Data Protection Lead who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.
This version September 2022
Due for review September 2024

Easthall Park Housing Cooperative Ltd

Information Security Procedure

Introduction

Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation. It may include personal information about a living individual, or it may be required for the running of EPHC's business. EPHC is committed to ensuring that all personal data will be processed in accordance with best data security practice and the UK General Data Protection Regulation (UK GDPR).

Purpose

The purpose and objective of this Information Security Policy is to protect EPHC's information assets from all threats, whether internal or external, deliberate or accidental, to protect personal and business information, ensure business continuity and minimise business damage by ensuring that all EPHC personnel understand our requirements for handling personal data and to clarify the standards of data security which we expect to be implemented.

Information will be protected from a loss of:

- Confidentiality: ensuring that information is accessible only to authorised individuals
- Integrity: safeguarding the accuracy and completeness of information and processing methods, and
- Availability: ensuring that authorised users have access to relevant information when required

Responsibility for data security

This policy applies to all EPHC personnel.

All EPHC personnel have a responsibility to apply adequate security to personal data which they handle to prevent it from being unlawfully accessed, lost, wrongfully deleted or damaged and to comply with this policy. The Directors of EPHC are responsible for overseeing this Information Security Policy and, as applicable, developing related policies, procedures and guidelines.

Personal Data

Personal data means information which relates to a living individual who can be identified either from that information alone or when that information is combined with other information.

Security Measures

EPHC is committed to protecting the integrity of the information we hold. A data security breach could have a very serious legal, financial and reputational impact for the business.

Training

Appropriate training will be made available for existing EPHC personnel who have responsibility for handling personal data. Each new employee will be made aware of their obligations for data protection during their induction to the organisation. Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that EPHC personnel are adequately trained.

Compliance

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the organisation's disciplinary policy.

INFORMATION SECURITY PROCEDURES:

All EPHC personnel must adhere to the following procedures to ensure security of EPHC's personal data:

Use of Hardware and systems

Our systems have been designed to enable you to work effectively and securely, and you are expected to use them in a professional manner by:

- Using a strong password which must contain
- Never sharing passwords
- Never sharing devices
- Locking screens and mobile devices when not in use and ensuring they are physically secure
- Ensuring anti-virus is kept up to date
- Not downloading unauthorised software or applications onto any of our hardware
- Not connecting unauthorised devices or equipment (including USB sticks, printers etc…) to our devices or systems
- Not connecting to our systems over unsecured wi-fi

E-Mails

- You should be diligent when using email to ensure that you do not provide unauthorised access to our information, spread viruses or infect our systems with malware.

- Do not click on hyperlinks or open attachments in emails unless you trust the sender

- Encrypt any documents containing special categories of personal data before sending by email

- Double check the recipients before hitting "Send"

Your company email account remains the property of EPHC and we may monitor it from time to time to ensure compliance with this policy.

Printing

Care must be taken when printing including:

- Only print documents for which you absolutely need a hard copy
- Ensure all printing is collected from printers immediately
- Any printing remaining on a printer at the end of the day must be shredded

Storage of hard copy documents

Any hard copy (paper) documents containing personal data must be stored in a locked desk or cupboard with limited access. Any keys for accessing these areas must also be stored securely.

When a document containing personal data is no longer required it should be shredded. ONLY documents that do not contain personal data or sensitive information should be put in general waste or recycling bins.

Protecting Information when travelling

In addition to the measures set out above, particular care must be taken to prevent disclosure of information when out of the office. Avoid situations where others can read your documents (e.g., over your shoulder when on public transport) – if in doubt do not read such documents in public. If you are using a laptop in a public area you must use a privacy screen to reduce the chance of someone being able to read the contents of your screen.

Clear desk

All EPHC personnel are to leave their desk/workstation paper free at the end of the day.

All EPHC personnel are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals.

All office managers should have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

EPHC personnel should make sure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information, if needed to be printed, should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that EPHC personnel securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

All EPHC personnel are to leave their desk/workstation paper free at the end of the day and failure to comply with this instruction, could result in disciplinary action being taken.

Printers and fax machines should be treated with the same care.

Clear screen

All EPHC personnel are expected to log off from their PCs/ laptops when left for long periods and overnight. When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Windows key and 'L'. The company system does this automatically after 15 minutes, however taking this measure will reduce any security risk even further.

Mobile devices through which access to the network can be obtained, for example PDAs, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use. EPHC's personnel should also refer to the company's Bring Your Own Device (BYOD) policy.

EPHC personnel should make sure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Reporting a security breach

If you suspect that a security breach has or may occur you must report it immediately to Data Protection Lead.

What to do if you wish to complain about our approach to data security

If any party involved wishes to complain about our approach to Data Security, they should refer to Data Protection Lead who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Company Directors.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.
This version September 2022
Due for review September 2024

Clear Desk and Clear Screen Policy

Clear Desk

All Easthall Park Housing Cooperative personnel are to leave their desk/workstation paper free at the end of the day.

All Easthall Park Housing Cooperative personnel are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives;

All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins;

Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals.

All office managers should have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

Easthall Park Housing Cooperative personnel should make sure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information, if needed to be printed, should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that Easthall Park Housing Cooperative personnel securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

All Easthall Park Housing Cooperative personnel are to leave their desk/workstation paper free at the end of the day and failure to comply with this instruction, could result in disciplinary action being taken.

Printers and fax machines should be treated with the same care.

Clear Screen

All Easthall Park Housing Cooperative personnel are expected to log off from their PCs/ laptops when left for long periods and overnight. When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Windows

key and ‘L’. The company system does this automatically after a given time, however taking this measure will reduce any security risk even further.

Mobile devices through which access to the network can be obtained should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use. Easthall Park Housing Cooperative personnel should also refer to the Bring Your Own Device Policy.

Easthall Park Housing Cooperative personnel should make sure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Care must be taken that screens are not sited such that the information displayed on them can easily been seen by unauthorised persons.

Cameras or other recording devices must not be used in the vicinity of screens which may display sensitive date.

Dated	8.9.22
Document Owner	A Ali
Approved By	Committee
Review Date	October 2024

Easthall Park Housing Cooperative

BRING YOUR OWN DEVICE (BYOD) POLICY

1. PURPOSE OF THIS DOCUMENT

This policy details acceptable use by Users whilst using their own Devices for the processing, which includes but is not not limited to, accessing, viewing, modifying and deleting of data held by our Organisation. It also details acceptable use by Users for accessing our organisation's systems where the User's role requires them to access such data whilst away from their place of work or as otherwise approved by the Organisation.

2. DEFINITIONS

BYOD – Bring Your Own Device	Refers to Users using their own Device or systems (which are not owned or provided by the Organisation) or applications to access and store the Organisation's information, whether at the place of work or remotely, typically connecting to the company's Wireless Service or VPN.
Data Controller	The Data Controller is a person, group or organisation that alone or jointly with others determines the purposes and means of the processing of personal data.
Device	An electronic device recognised as a BYOD, including systems and applications used on such a device.
User	A member of staff, employee, contractor, visitor, volunteer, stakeholder or other person authorised to access and use the Organisation's systems.

3. POLICY INTRODUCTION

This policy covers the use of electronic Devices not owned/issued by the Organisation which could be used to access corporate systems and process data, alongside their own data. Such Devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

If Users wish to use Devices to access organisational systems, data and information, Users may do so provided that they follow the provisions of this policy and the advice and guidance provided through the IT Department.

It is the Organisation's intention to place as few technical and policy restrictions as possible on BYODs, subject to the Organisation meeting its legal obligations, including, but not limited to its legal compliance requirements with regards to data protection law.

The Organisation, as the Data Controller, remains in control of the data regardless of the ownership of the Device. Users are required to keep any information and data belonging to the Organisation securely. This applies to information held on a User's Device, as well as on the Organisation's systems. Users are required to assist and support the Organisation in carrying out its legal and operational obligations, including co-operating with the IT

Department should it be necessary to access or inspect data belonging to the Organisation stored on a Device.

The Organisation reserves the right to refuse, prevent or withdraw access to Users and/or particular Devices or software where it considers that there are unacceptable security or other risks including but not limited to its staff, employees, business, reputation, systems or infrastructure.

4. SYSTEM, DEVICE AND INFORMATION SECURITY

The Organisation takes information and systems security very seriously and invests significant resources to protect data and information in its care. The use of a User's Device must adhere to the organisation's policies with regard to security and compliance with data protection law. In particular, where a User uses a Device as a work tool, Users must maintain the security of the Organisation's data and information which a User processes (which includes, but is not limited to, viewing, accessing, storing or deleting information and data belonging to the Organisation).

From time to time, the Organisation may require that Users install or update approved device management software on their Device.

It is the User's responsibility to familiarise themselves with the Device sufficiently to keep data secure. In practice, this means:

a) preventing the theft and loss of data (using for example Biometric/PIN/Password/Passphrase locks and in accordance with other organisational policies and procedures relating to security and data protection law);
b) keeping information confidential, where appropriate; and
c) maintaining the integrity of data and information.

Users must never retain personal data from the Organisation's systems on their Device. If Users are in any doubt as to whether particular data can be stored on a Device, Users are required to err on the side of caution and consult their manager or seek advice from the IT Department.

Users must at all times:

a) use the Device's security features, such as a Biometric, PIN, Password/Passphrase and automatic lock to help protect the device when not in use.
b) keep the Device software up to date, for example using Windows Update or Software Update services.
c) activate and use encryption services and anti-virus protection if a User's Device features such services.
d) install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the Device has this feature.
e) remove any information and data belonging to the Organisation stored on a User's Device once a User has finished with it, including deleting copies of attachments to emails, such as documents, spreadsheets and data sets.
f) limit the number of emails and other information that Users are syncing to the Device to the minimum required, for example only keep the past 24 hours of email in sync.
g) remove all information and data belonging to the Organisation from the Device and return it to the manufacturers' settings before a User sells, exchanges or disposes of the Device.

h) Upon leaving the Organisation, such as at termination of contract of employment, the Device owner must allow the Device to be audited and all information and data belonging to the Organisation be removed, if requested to do so by the Organisation.

5. LOSS OR THEFT

In the event that a Device is lost or stolen or its security is compromised, Users must promptly report this to the IT Department, in order that they can assist Users to change the password to all organisational services.

It is also recommended that Users also do this for any other services that have accessed via that Device, e.g. social networking sites, online banks, online shops). Users must also cooperate with the IT Department in wiping the device remotely, even if such a wipe results in the loss of User's own data, such as photos, contacts and music.

The Organisation will not monitor the content of User's personal Devices. However the IT Department reserves the right to monitor and log data traffic transferred between a User's Device and Organisational systems, both over internal networks and entering the Organisation via the Internet.

In exceptional circumstances, for instance where the only copy of a document belonging to the Organisation resides on a personal Device, or where the Organisation requires access in order to comply with its legal obligations (e.g. it is obliged to do so by a Court of Law or other law enforcement authority) the Organisation will require access to data and information owned by the Organisation stored on a User's personal Device. Under these circumstances, all reasonable efforts will be made to ensure that the Organisation does not access User's private information.

Users are required to conduct work-related, online activities in line with the Organisations's policies and procedures. This requirement applies equally to BYOD.

6. SUPPORT

The Organisation takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding BYOD Devices, or for any loss or damage resulting from support and advice provided.

7. USE OF PERSONAL CLOUD SERVICES

Personal data as defined by the Data Protection Act 2018 and UK GDPR and confidential information and data belonging to the Organisation may not be stored on personal cloud services (e.g. One Drive / Dropbox etc.)

8. COMPLIANCE AND DISCIPLINARY MATTERS

All Users must comply with this policy, and failure to do so may constitute grounds for action, in accordance with the Organisation's Disciplinary Policy.

9. WHAT TO DO IF YOU WISH TO COMPLAIN ABOUT OUR BRING YOUR OWN DEVICE POLICY?

If any User or potential User wishes to complain about our approach to BYOD they should refer to our Data Protection Lead who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

10. REVIEW CYCLE

Date of this version September 2022
Due for Review September 2024.

Appendix 4 data protection policy

Easthall Park Housing Cooperative

Data Subject Rights Procedures

Introduction

The UK General Data Protection Regulation (UK GDPR) provides all living individuals (data subjects) with certain rights over their personal data. Not all rights are absolute, and some can be subject to exemptions.

This Procedure should be read in conjunction with the Data Protection Policy.

Purpose

The purpose of this procedure is to explain how a data subject can make a rights request in relation to their personal data, as defined in Article 15 to 21 of the GDPR, and how Easthall Park Housing Cooperative will handle requests to ensure compliance with the GDPR and any other relevant legislation.

Where personal data is being processed by Easthall Park Housing Cooperative and the identity of the data subject has been verified, Easthall Park Housing Cooperative will respond to the request and provide the data subject with a response within the obligated timeframe.

Scope

This procedure applies to all Directors, Associates, members, employees (temporary and permanent), volunteers, tenants and other external data subjects (referred to herein as 'Easthall Park Housing Cooperative data subjects').

The following rights involving personal data are covered:

Data Subject Right	GDPR Article
Right of Access (Subject Access Request)	Article 15
Right of Rectification	Article 16
Right of Erasure (Right to be forgotten)	Article 17
Right to restrict processing	Article 18
Right of transfer data (Data Portability)	Article 20
Right to object to processing	Article 21

Responsibilities

All Easthall Park Housing Cooperative personnel, are responsible for adhering to this procedure.

The nominate EPHA data protection officer, RGDP, is responsible for maintaining a register of all rights requests and co-ordinating the collection of personal data and providing any required responses.

Definition of Personal Data

Personal data, for the purposes of this procedure is defined as, any information relating to an identified or identifiable living individual who can be identified, directly or indirectly. Personal data includes facts, opinions or intentions relating to the data subject.

The UK GDPR applies to personal data which is:

- processed wholly or partly by automated means e.g., IT system, CCTV, voicemail forms; or
- intended to form part of a filing system e.g., categorised file that enables personal data to be readily accessible.

Receiving a Valid Request

A data subject can make a request via any method and personnel should always be aware of requests via the following:

Verbal Requests	Email	Fax
Written (letter)	Social Media	Website Contact Forms

A request cannot be progressed if we do not have enough information to clearly locate and identify the personal data within the request. The data subject can be asked for further information in order to help locate the information.

Verifying the Identity of the Data Subject

Where there are any reasonable doubts concerning the identity of the data subject, additional information will be requested to confirm the identity of the data subject.

Once Easthall Park Housing Cooperative is satisfied, a note will be made that this requirement has been met and any copies of identification documents will be shredded (there is no requirement to retain copies of any ID verification). Any originals will be sent back via recorded delivery.

If Easthall Park Housing Cooperative can demonstrate that it is not able to identify the data subject, even after additional information is provided, a refusal notice to act upon the request will be issued.

Requests from parties other than the data subject

There are occasions where a data subject may agree to a third party making a request on their behalf, such as a solicitor or family member.

To protect a data subject's personal data, Easthall Park Housing Cooperative will make all the necessary checks to be satisfied that the individual making the request on behalf of the data subject is entitled to do so. This may include requesting a written authority to make the request (e.g., evidence of consent from the individual) or a more general power of attorney.

No information will be released until Easthall Park Housing Cooperative is satisfied. Easthall Park Housing Cooperative may feel it appropriate to contact an individual directly to discuss the request, for example, if asked to release special category data.

In the event of this, the data subject will be given an overview of the type of information that will be released and the option to:

- view their personal data first and upon consent it will be released to the third party
- grant permission for it to be sent directly to the third party
- withdraw consent and no information will be sent to the third party

Charges

In most cases there will be no fee charged for responding to a request, however where Easthall Park Housing Cooperative can demonstrate that the request is manifestly unfounded or excessive in nature it can either:

- charge a reasonable fee, reflective of the administrative costs of dealing with the request; or
- refuse to act on the request.

A data subject will be informed of such decision, the reason why and how a complaint can be raised with the Information Commissioner's Office (ICO) if they wish to appeal.

If the request relates to access to personal data, where Easthall Park Housing Cooperative has provided one copy of the personal data free of charge, for further copies of the same data, Easthall Park Housing Cooperative shall charge a reasonable fee to the data subject based on administrative costs.

Timescales

Easthall Park Housing Cooperative shall provide a response to the data subject without undue delay and in any event within one month of receipt of a valid request. The day the request is received is day one (for example, if the request is received on 10th August the last day for responding is 10th September). Where there is no corresponding date in the following month the last day of that month will be the last date for responding (e.g., received on 31st August the last day will be 30th September).

This period may be extended by two further months, considering the complexity and number of the requests.

The nominate EPHA data protection officer, RGDP, shall inform the data subject of any extension within one month of receipt of the request, together with the reasons for the delay.

If it is not possible to action the request of the data subject, The nominate EPHA data protection officer, RGDP, shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not progressing and of the possibility of complaining to the ICO.

Responding to Requests

The data in any response shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Where an email or online request for copy data is received, the data shall be provided by email, unless the data subject has requested that it be provided in another form. Any such personal data which is emailed shall be encrypted and subject to appropriate security measures.

Access Requests (Subject Access Requests)

This right enables a data subject to verify that Easthall Park Housing Cooperative is lawfully processing their personal data and to check its accuracy. Where data is being processed by Easthall Park Housing Cooperative and the data subject makes a request to access the data, Easthall Park Housing Cooperative shall provide the data subject with access to the personal data and provide:

- the purpose of the processing;
- the categories of personal data being processed;
- the recipients or categories of recipients to whom we have disclosed or will disclose personal data;
- the retention period for the data (or how we determine that);
- the existence of the right to have us rectify, erase or restrict processing of that data;
- the right to lodge a complaint with the ICO;
- the source of the information if we have not collected the data direct from the subject; and
- the existence of any automated decision making.

Where personal data is transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer.

Easthall Park Housing Cooperative has a duty to ensure other individual's information is treated fairly or protected accordingly. Therefore, before Easthall Park Housing Cooperative releases anything to the data subject or representative it has to

ensure that it's not inappropriately releasing information about another individual who can be identified from that information.

On occasions where somebody else can be identified from that information, Easthall Park Housing Cooperative will not release data relating to the data subject unless the other individual has consented to the release of the information or it is reasonable in all circumstances to release the information without consent.

Easthall Park Housing Cooperative will take the below approach:

- Seek documented consent from other individuals
- Where appropriate redact information so other individuals cannot be identified, such as names / addresses/ identification
- Where appropriate provide a summary of the personal data
- Review whether it would be reasonable to release the information without consent, considering;
- is the information already known by the data subject?
- is the individual acting in their professional capacity and had dealings with the data subject?
- is there a duty of confidentiality owed to the other individual?

The data subject's interests and that of the other individual will be reviewed and considered.

All decisions will be made on a case-by-case basis, taking into consideration other legislation that may force the release of information to the data subject.

The Data Protection Act 2018 makes it an offence to intentionally alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

Rectification Requests

Where the request is for the rectification of inaccurate personal data, Easthall Park Housing Cooperative will restrict further processing of personal data whilst verifying the accuracy.

Where the rectification request is upheld, Easthall Park Housing Cooperative shall inform any third parties who have been sent personal data that the data subject has made a rectification request and instruct all parties what rectification is required.

The exception to notifying third parties is if this proves impossible or involves disproportionate effort.

Erasure Requests

When requested to do so by the data subject, Easthall Park Housing Cooperative will erase personal data without undue delay where the request does not conflict with any legal, regulatory or other such constraints.

This right can only be exercised by data subjects where:

(a) the personal data is no longer necessary in relation to the purpose for which it was collected or processed;
(b) where the data subject's consent to processing is withdrawn;
(c) where the data subject objects to the processing and there are no overriding legitimate grounds for processing;
(d) where there is no legal basis for the processing; or
(e) where there is a legal obligation to delete data.

Where personal data is to be deleted, data held in different locations and in different formats will be reviewed to ensure that all relevant personal data is erased.
Where we have made any personal data public, we shall take reasonable steps (taking into account technology and cost) to notify other controllers processing the data of the data subject's request for erasure.

Easthall Park Housing Cooperative is not required to and will not delete personal data where the processing carried out is necessary for:

(a) exercising the right of freedom of expression;
(b) complying with a legal obligation in the public interest or in the exercise of an official authority;
(c) for public health reasons;
(d) for archiving purposes; or
(e) for the establishment, exercise or defence of legal claims.

Once the relevant personal data has been deleted the data subject shall be advised that the data has been erased unless doing so is impossible or involves disproportionate effort.

Restriction Requests

The data subject shall have the right to restrict (block) processing of their personal data.

This is not an absolute right and the data subject will only be entitled to restriction where:

(a) the accuracy of personal data is contested by the data subject for a period to enable us to verify the accuracy;
(b) the processing is unlawful, and the data subject does not want it to be erased but requests restriction instead;
(c) we no longer need the data for the purpose of the processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims; or

(d) the processing has been objected to and verification of that objection is pending.

Where the data subject exercises their right to restriction, personal data can then only be processed with their consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another person or legal entity or for reasons of important public interest of the UK or an EU Member State.

Where we have restricted any form of processing and that restriction is subsequently to be lifted, we shall advise the data subject accordingly unless doing so is impossible or involves disproportionate effort.

Transfer Requests (Data Portability)

This right allows a data subject to obtain and reuse personal data for their own purposes across different services.

Where a data subject requests a copy of their personal data for the purposes of transferring it from Easthall Park Housing Cooperative to another data controller we shall do so provided:

(a) the legal basis for processing is based on consent or a contract with the data subject; and
(b) the processing is carried out by automated means.

The data subject shall only be provided with the personal data they have provided to Easthall Park Housing Cooperative and the personal data gathered by us in the course of our dealings with the individual or which has been generated from our monitoring of the data subject's activity. This will only be data held electronically.

The data subject is entitled to be provided with their personal data in a structured, commonly used and machine-readable format for transfer to another controller; or where possible to have Easthall Park Housing Cooperative transfer the data direct to another controller.

Objection Requests

A data subject can object to the processing of their personal data, including profiling, on grounds relating to their particular situation. Where a request is received, Easthall Park Housing Cooperative is under an obligation to act upon a request where one of the following conditions applies:

- where their personal data is processed based on the public interest or in the exercise of official authority; or
- where we are processing their personal data based on legitimate interests.

If we can demonstrate that Easthall Park Housing Cooperative has legitimate grounds for the processing which override the interests, rights and freedoms of the

data subject or for the establishment, exercise or defence of legal claims, it is not necessary to cease processing.

This does not apply to direct marketing. Data subjects are entitled to object to direct marketing (in any form) which is sent to them. This is an absolute right and where such a request is received, Easthall Park Housing Cooperative must comply with the request.

Applying Exemptions

The UK Data Protection Act 2018 provides exemptions which enable organisations not to respond to data subject rights in certain circumstances.

Easthall Park Housing Cooperative may be exempt from compliance with the data subject rights if certain exemptions apply. Careful consideration should be given to these exemptions and whether they apply before responding to any request by a data subject. Advice from the Data Protection Officer or legal adviser is recommended. The exemptions for compliance with the request are set out in schedule 2 parts 1, 2 and 3 of the Data Protection Act 2018.

In summary these are:

- **Crime and taxation** – for the prevention or detection of crime; the apprehension or prosecution of offenders or the assessment or collection of tax or duty or an imposition of a similar nature to the extent that those provisions would prejudice the activity.

- **Immigration** – for the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control.

- **Information required to be disclosed by law etc. or in connection with legal proceedings** – to the extent that the application of the provisions would prevent same including disclosure which is necessary for the purpose of or in connection with legal proceedings (including prospective legal proceedings) or for obtaining legal advice or otherwise establishing, exercising or defending legal rights.

- **Functions designed to protect the public** – certain functions carried out to protect the public from financial loss through fraud etc.; to protect charities; for health and safety reasons; to prevent malpractice in a public office; or to protect business interests.

- **Regulatory activity** – relating to certain bodies where the application of the provisions would prejudice the discharge of their function.

- **Legal professional privilege/confidentiality of communications** – some solicitor/client communications or information prepared for the purpose of litigation

- **Self-incrimination** – to the extent that complying would reveal evidence of an offence

- **Corporate finance** – in certain circumstances

- **Management forecasts** - to the extent that the application of the provisions would prejudice the conduct of the business or activity concerned

- **Negotiations** - with the data subject to the extent that the application of the provisions would prejudice those negotiations

- **Confidential references** - given to or provided by Easthall Park Housing Cooperative

- **Health, social work, education and child abuse data** to the extent that the application of the provisions would cause prejudice.

If we apply any exemptions or refuse the request for any reason, we will provide the data subject with the following information:

- the reasons why the request is refused/exemptions applied
- their right to make a complaint to the ICO
- their ability to seek to enforce this right through judicial remedy

Register of Requests

The nominate EPHA data protection officer, RGDP, is responsible for maintaining a register of requests, to allow monitoring of the progress of requests and the volume of requests received.

Records Retention

A copy of all the data retrieved must be taken for reference should the data be challenged by the data subject. These will be maintained in line with the records retention schedule and retained for 1 year.

Complaints / Right to appeal

If the data subject or their representative is not satisfied with the outcome of their rights request, in the first instance, the individual will be encouraged to contact the nominate EPHA data protection officer, RGDP, If they are still not satisfied, they can contact the Information Commissioner's Office directly at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel:
E-mail: casework@ico.org.uk
Website: www.ico.org.uk

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the nominate EPHA data protection officer, RGDP, to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the EPHA data protection lead and/or committee.

Policy Review
This policy will be reviewed every 24 months or when required to address any weakness in the procedure or changes in legislation or best practice.

Dated	8.9.22
Document Owner	A Anila
Approved By	Committee
Review Date	June 24

Data Protection Impact Assessment Procedure

Please read this document before completing the DPIA template, contained within the Appendix

Contents

Overview

A Data Protection Impact Assessment ('DPIA') is a tool to help us identify and minimise the data protection risks of new projects. They are part of our accountability obligations under the UK General Data Protection Regulation, and an integral part of the 'data protection by default and by design' approach.

We must do a DPIA for certain types of processing of personal data, or any other processing that is likely to result in a high risk to individuals.

A DPIA must:

1. describe the nature, scope, context and purposes of the processing;
2. assess necessity, proportionality and compliance measures;
3. identify and assess risks to individuals; and
4. identify any additional measures to mitigate those risks.

To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Data Protection Lead will be consulted when completing a DPIA and where appropriate, individuals and relevant experts. Any data processors may also need to assist in completing it.

If we identify a high risk that we cannot mitigate, we must consult the Information Commissioner's Office ('ICO') before starting the processing.

An effective DPIA helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

This procedure explains the principles and process that form the basis of a DPIA. It helps us to understand what a DPIA is for, when we need to carry one out, and how to go about it.

What is a DPIA?

A DPIA is a process designed to help us systematically analyse, identify and minimise the data protection risks of a project or planned change. It is a key part of our accountability obligations under the UK GDPR, and when done properly helps us assess and demonstrate how we comply with all of our data protection obligations.

It does not have to eradicate all risk, but should help us minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

DPIAs are designed to be a flexible and scalable tool that we can apply to a wide range of projects regardless of size. Conducting a DPIA does not have to be complex or time-

consuming in every case, but there must be a level of strictness in proportion to the privacy risks arising.

Why are DPIAs Important?

DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to £10 million or 2% annual turnover.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations. However, DPIAs are not just a compliance exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and Easthall Park Housing Cooperative

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used.

Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information.

In turn, this can create potential benefits for our reputation and relationships with individuals:

- help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations;
- identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on; and
- reduce the ongoing costs of a project by minimising the amount of information we collect where possible and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within Easthall Park Housing Cooperative and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a '**data protection by design'** approach.

How are DPIAs Used?

A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA done by the product developer to inform our own DPIA on our implementation plans.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it's important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point

when there is a realistic opportunity to influence those plans. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of a DPIA back into any project plan. We should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help us manage and review the risks of the processing and the measures put in place on an ongoing basis. We need to keep it under review and reassess if anything changes. In particular, if we make any significant changes to how or why you process personal data, or to the amount of data we collect, we need to show that our DPIA assesses any new risks.

An external change to the wider context of the processing should also prompt us to review our DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing we do or the vulnerability of a particular group of data subjects.

What Kind of 'Risk' do DPIAs Assess?

There is no explicit definition of 'risk' in the UK GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The UK GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

When do we Need to do a DPIA?

We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you **must** do a DPIA if you plan:

Systematic and extensive profiling with significant effects:
"any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".

Large scale use of sensitive data:
"processing on a large scale of special categories of data referred to in Article 9(1) (See Appendix 2) or of personal data relating to criminal convictions and offences referred to in Article 10"

Public monitoring:
"a systematic monitoring of a publicly accessible area on a large scale".

The ICO has also published a list of the kind of processing operations that are likely to be high risk and also **require** a DPIA.

New technologies: processing involving the use of new technologies, or the novel application of existing technologies (including AI). **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
Large-scale profiling: any profiling of individuals on a large scale.
Biometrics: any processing of biometric data.
Genetic data: any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.
Data matching: combining, comparing or matching personal data obtained from multiple sources.
Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
Targeting of children or other vulnerable individuals: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
Risk of physical harm: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

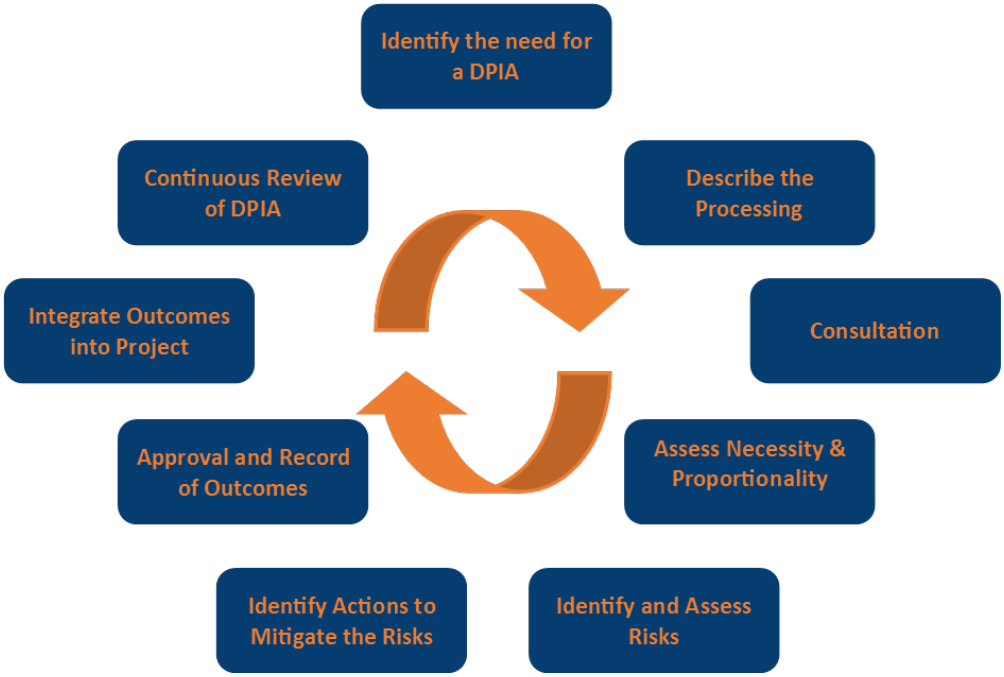
We should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving any use of personal data.

When deciding whether to do a DPIA, we should first answer the screening questions at Appendix 1.

After answering the screening questions, if the decision is made that a DPIA is needed, use the following guidance, as you go along, to complete the DPIA template at Appendix 3.

How to complete a DPIA

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



Responsibility for completing a DPIA

The project manager / lead would usually be best placed to conduct the required DPIA along with any other stakeholders who are able to input into the process.

The Data Protection Lead/DPO will have a significant role in supporting the process, providing advice and guidance, will approve any completed assessment and where required liaise with the Information Commissioners Office.

Step 1: Identify the need for a DPIA

1.1 Contact the Data Protection Lead /DPO and advise them of the new project/change.

1.2 Complete the DPIA Initial Screening Form (Appendix 1) to determine if you need to complete a DPIA.

1.3 If you decide that you do not need to do a DPIA, you should document the decision and the reasons for it on the DPIA Initial Screening Form (Appendix 1).

1.4 If you need to complete a DPIA you should use the DPIA Template (Appendix 3) and complete Step 1, where you should list the types of processing identified from the screening form, the aims of the project and why the need to complete a DPIA was identified.

Jump to Step 1 of the template

Step 2: Describe the Processing

2a Describe how and why you plan to use the personal data

The description must include “the nature, scope, context and purposes of the processing”. The nature of the processing is what you plan to do with the personal data.

This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether there are any data processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

2b The scope of the processing is what the processing covers.

This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

2c The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact.

This might include, for example:

- the source of the data;
- the nature of the relationship with the individuals (tenants, staff);
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern.

2d The purpose of the processing is the reason why you want to process the personal data.

This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole

Jump to Step 2 of the template

Step 3: Consultation

You should always seek the views of individuals (or their representatives) unless there is a good reason not to.

In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of the DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

Do you need to consult anyone else?

If the project involves a **data processor**, you may need to ask them for information and assistance.

You should consult all relevant internal stakeholders, the **IT Support Provider** if this is a new system or change to an existing system to allow Information Security to be considered.

In some circumstances we might also need to consult the ICO once you have completed your DPIA. (Explained in Step 6)

Jump to Step 3 of the template

Step 4: Assess Necessity and Proportionality

You should consider:

- Do your plans help to achieve your purpose?

- Is there any other reasonable way to achieve the same result?

The Article 29 guidelines also say you should include how you ensure data protection compliance, which are a good measure of necessity and proportionality.

In particular, you should include relevant details of:

- your lawful basis for the processing; (see Appendix 2 - Conditions of Processing)
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals' rights;
- measures to ensure your processors comply; and
- safeguards for any international transfers.

Jump to Step 4 of the template

Step 5: Identify and Assess Risks

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material.

In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). You may wish to discuss these with the IT Provider for electronic data transfers.

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

The below Risk Matrix must be considered when assessing likelihood and severity of harm to the rights and freedoms of the individual.

Severity of harm				
	Serious harm	Low risk	High risk	High risk
	Some harm	Low risk	Medium risk	High risk
	Minimal harm	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Jump to Step 5 of the template

Step 6: Identify Actions to Mitigate the Risks

Against each risk identified, record the source of that risk.

You should then consider options for reducing that risk.

For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.

Record whether the measure would reduce or eliminate the risk.

You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of ‘residual risk’ after taking additional measures; and

- whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.

When to Consult the ICO

If you have identified a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so. The focus is on the 'residual risk' after any mitigating measures have been taken. If the DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

How do we consult the ICO?

The DPO will consult with the ICO on Easthall Park Housing Cooperative 's behalf. This is done by completing the online form.

The submission must include:

- a description of the respective roles and responsibilities of any joint controllers or processors;
- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- a copy of the DPIA;

We will be notified if the DPIA has been accepted for consultation within ten days of sending it. If the ICO agree that a DPIA was required, they will review the DPIA.

They will consider whether:

- the processing complies with data protection requirements;
- risks have been properly identified; and
- risks have been reduced to an acceptable level.

The ICO will provide a written response, advising that:

- the risks are acceptable and you can go ahead with the processing;
- you need to take further measures to reduce the risks;
- you have not identified all risks and you need to review your DPIA;
- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed.

In some cases, the ICO may take more formal action. This might include an official warning not to proceed, or imposing a limitation or ban on processing.

If we disagree with the ICO advice we can ask for a review of the decision.

Jump to Step 6 of the template

Step 7: Approval and Record of Outcomes

As part of the approval process, you should submit your assessment to the Named Role/DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.

Jump to Step 7 of the template

Step 8: Integrate Outcomes into Project

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

It is good practice to publish DPIA's to aid transparency and accountability. This could help foster trust in our processing activities, and improve individuals' ability to exercise their rights.

Step 9: Continuous Review of DPIA

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

.

Appendix 1 - DPIA Initial Screening Form

1. Project Details

Project Title / Change Description:	
Project Manager/ Lead details:	
Date of Screening:	

2. Answer yes or no to all the different types of processing listed below

Does the processing you are planning:	**Answer**
Use systematic and extensive profiling or automated decision making to make significant decisions about people?	
Process special category data (see Appendix 2) or criminal offence data on a large scale?	
Systematically monitor a publicly accessible place on a large scale?	
Use new technologies?	
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	
Carry out profiling on a large scale?	
Process biometric or genetic data?	
Combine, compare or match data from multiple sources?	
Process personal data without providing a privacy notice directly to the individual?	
Process personal data in a way which involves tracking individuals' online or offline location or behaviour?	
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	
Process personal data which could result in a risk of physical harm in the event of a security breach?	

3. If the answer is **yes** to any one of these types of processing, then you **must** complete a DPIA. If the answer was **no** to all these types, then you must review the following processing listed below that may require a DPIA

Does the processing involve:	**Answer**
Evaluation or scoring	
Automated decision-making with significant effects	
Systematic monitoring	
Processing of sensitive data or data of a highly personal nature	
Processing on a large scale	
Processing of data concerning vulnerable data subjects.	
Innovative technological or organisational solutions	

Processing involving preventing data subjects from exercising a right or using a service or contract.	

4. If the answer is **yes** to any of these processing types you must discuss the requirement to complete a DPIA with the Data Protection Lead/DPO.

Is DPIA Required?	
Reason for Decision if not completing DPIA:	

If the decision is made that a DPIA is needed, use the above guidance to complete the DPIA template at Appendix 3.

Appendix 2 – Conditions for Processing

Below are the different legal bases available for processing personal data and special categories of data.

Legal Bases for Processing Personal Data:

- 6(1)(a) – Consent of the data subject *(only use consent if there is no other condition that can be used)*
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Categories of Special Category Data:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life and sexual orientation
- Genetic data
- Biometric data used to identify an individual

Conditions for Processing Special Categories of Data:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-pro fit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in

connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 3 -DPIA Template

Data Protection Impact Assessment

For guidance on how to complete this form, it is important to read the above DPIA Procedures before and during completion of this assessment.

This assessment must be commenced at the beginning of any project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes must be integrated back into the project plan.

Name of Organisation	
Project Title / Change Description:	
Project Manager/ Lead details:	
Name of Data Protection Officer	
Date of Assessment:	

Step 1: Identify the need for a DPIA
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project scoping. Summarise why you identified the need for a DPIA. (See DPIA Procedure Step 1 for further guidance).

Step 2: Describe the Processing
2a Describe the nature of the processing: (See DPIA Procedure Step 2 for further guidance)
How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone?

What types of processing identified as likely high risk are involved?
Insert flow diagram showing data flows (optional)

2b Describe the scope of the processing:
(See DPIA Procedure Step 2 for further guidance)

Details of personal data

Please indicate what personal data will be collected/stored/processed, please indicate with an X where applicable.

Administration data

Name	☐
Date of Birth/Age	☐
Gender	☐
Contact details	☐
Unique identifier e.g. student number/NI No.	☐
Other data (please specify):	

Special Categories of data

Racial or ethnic origin	☐
Political opinion	☐
Religious or philosophical beliefs	☐
Trade Union membership	☐
Physical or mental health condition	☐
Sexual life and sexual orientation	☐
Genetic data	☐
Biometric data used to identify an individual	☐

Other sensitive information

Financial information/bank account details	☐
Criminal convictions and offences	☐
Other (please specify):	

Under Article 6 of the UK GDPR one of the following conditions needs to apply before the processing of personal data is lawful. Please indicate which condition applies: (See Appendix 2)

- The individual who the personal data is about has given/will give unambiguous consented to the processing
  ☐
- The processing is necessary for the performance of a contract with the individual
  ☐
- The processing is necessary for a legal obligation
  ☐
- The processing is necessary for the vital interests of someone (i.e. life or death situation)
  ☐
- The processing is carried out in the public interest or in the exercise of official authority
  ☐
- The processing is in the legitimate interests of the business or another party and does not prejudice the rights and freedoms of the individual (please provide further details):
  ☐

If processing Special Category Data, please state which of the conditions for processing specified in Appendix 2 applies.

2c Describe the context of the processing:
(See DPIA Procedure Step 2 for further guidance)

What is the nature of your relationship with the individuals?

How much control will they have?

Would they expect you to use their data in this way?

Do they include children or other vulnerable groups?

Are there prior concerns over this type of processing or security flaws?

Is it novel in any way?

What is the current state of technology in this area?

Are there any current issues of public concern that you should factor in?

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

2d Describe the purposes of the processing:
(See DPIA Procedure Step 2 for further guidance)

What do you want to achieve?

What is the intended effect on individuals?

What are the benefits of the processing for you, and more broadly?

Step 3: Consultation

Consider how to consult with relevant stakeholders: (See DPIA Procedure Step 3 for further guidance)

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Who else do you need to involve within your organisation?

Do you need to ask any relevant data processors to assist?

Do you plan to consult information security experts, or any other experts?

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular:
(See DPIA Procedure Step 4 for further guidance)

What is your lawful basis for processing?

Does the processing actually achieve your purpose?

Is there another way to achieve the same outcome?

How will you prevent function creep?

How will you ensure data quality and data minimisation?

What information will you give individuals?

How will you help to support their rights?

What measures do you take to ensure data processors comply?

How do you safeguard any international transfers?

Step 5: Identify and Assess Risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. (See DPIA Procedure Step 5 for further guidance and Risk Matrix)	Likelihood of Harm	Severity of Harm	Overall risk
Risk No. 01			
Risk No. 02			

Step 6: Identify Actions to Mitigate the Risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5
(See DPIA Procedure Step 6 for further guidance)

Risk	**Actions to reduce or eliminate risk**	**Effect on Risk** *(reduced / eliminated*	**Residual Risk** *(Low/ Medium/ High)*	**Action Approved** *(Yes/No)*

		/ Accepted)		
Risk No. 01				
Risk No. 02				

Step 7: Approval and Record of outcomes

(See DPIA Procedure Step 7 for further guidance)

Item	Signed / Date	Notes
Risk Actions approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
This DPIA will be kept under review by:		*The Data Protection Lead should also review ongoing compliance with DPIA*

Data Protection Impact Assessment

Screening Procedure

This procedure is to be used when a new project, or a change to a project, which involves any processing of personal data is being planned. This can include, but is not exclusive to, new IT systems, marketing campaigns, sharing personal data with other website providers, initiatives involving uses of personal data in new ways.

What is a DPIA?
Data Protection Impact Assessments (DPIA) are a tool to help us identify and minimise the data protection risks of new projects. They are part of our accountability obligations under the General Data Protection Regulation, and an integral part of the 'data protection by default and by design' approach.

An effective DPIA helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

Why are DPIAs important?
Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk to the rights and freedoms of the people whose personal data is being processed (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to €10 million or 2% annual turnover.

How are DPIAs used?
A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA completed by the product developer to inform our own DPIA on our implementation plans.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it is important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point when there is a realistic opportunity to influence those plans.

What kind of 'risk' do DPIA's assess?
There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

When do we need to do a DPIA?
We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk, we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

When deciding whether to do a DPIA, we should first answer the screening questions at Appendix 1.

After answering the screening questions:-

1) if the decision is made that a DPIA is needed, contact the Data Protection Manager or DPO for guidance

or

2) if the decision is made that you do not need to carry out a full DPIA, you should complete the mini DPIA at Appendix 3 and this form should be saved in the main Project File and a copy sent to the Data Protection Manager and DPO.

Appendix 1 - DPIA Initial Screening Form

1. Project Details

Project Title / Change Description:	
Project Manager/ Lead details:	
Date of Screening:	

2. Answer yes or no to all the different types of processing listed below

Does the processing you are planning:	**Answer**
Use systematic and extensive profiling or automated decision making to make significant decisions about people? Includes: Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination Excludes: Processing with little or no effect on people	
Process special category data or criminal offence data on a large scale*? Includes: • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data	

• Trade Union membership data • Genetic data • Biometric data for the purpose of uniquely identifying a person • Health data • Sex life or sexual orientation data • Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data • Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive (*see Appendix 2)	
Systematically monitor a publicly accessible place on a large scale?* Includes processing used to observe, monitor or control people. (*see Appendix 2)	
Use new technologies? The work involves *significant innovation* or use of a *new technology.* Examples could include combining use of fingerprint and face recognition for improved physical access control; new "Internet of Things" applications.	
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	
Carry out profiling on a large scale?* (*see Appendix 2)	
Process biometric or genetic data?	
Combine, compare or match data from multiple sources?	
Process personal data without providing a privacy notice directly to the individual?	
Process personal data in a way which involves tracking individuals' online or offline location or behaviour?	
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	
Process personal data which could result in a risk of physical harm in the event of a security breach?	

3. If the answer is **yes to any one** of these types of processing, then you **must** complete a DPIA. If the answer was **no** to all these types, then you must review the following processing listed below that may require a DPIA

Does the processing involve:	**Answer**

Evaluation or scoring	
Automated decision-making with significant effects	
Systematic monitoring	
Processing of sensitive data or data of a highly personal nature	
Processing on a large scale	
Processing of data concerning vulnerable data subjects.	
Innovative technological or organisational solutions	
Processing involving preventing data subjects from exercising a right or using a service or contract.	

4. If the answer is **yes** to any of these processing types you must discuss the requirement to complete a full DPIA with the Data Protection Manager or DPO.

Is DPIA Required?	**Yes/No**
Reason for Decision if not completing DPIA: If you decide a full DPIA, is **not** required, you should now complete the Mini-DPIA at Appendix 3.	

Appendix 2

Definition of Special Category data:

Personal data relating to:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life and sexual orientation
- Genetic data
- Biometric data used to identify an individual

Definition of 'large scale':

The GDPR does not define what constitutes large-scale, however, the European Data Protection Board Article 29 Working Party, recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

- The number of data subjects concerned - either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity

- The geographical extent of the processing activity

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers

Examples that do not constitute large-scale processing include:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

Appendix 3

This form is to be used when you have considered the pre-screening questions in the Data Protection Impact Assessment (DPIA) procedure and decided that a full DPIA is **not** necessary. This includes where limited personal (not including special category) data is to be used for a new project/system or for replacement of a supplier of an existing system/service.

If you have not yet considered the pre-screening questions, you must do so before completing this form.

This form should be stored with the DPIA pre-screening form.

Mini-DPIA
Have you considered all the following Data Protection Principles:
Lawfulness, fairness and transparency
• What is the lawful basis you are relying on for the processing?
• Is this fair to the people whose data you are processing?
• Will the people whose personal data you are using expect their details to be used in this way (is this covered in your current relevant Privacy Notice)?
Purpose limitation
• What is the purpose of your proposal and why is it necessary to use personal data to achieve that purpose?
Data minimisation
• What is the minimum personal data necessary to achieve your purpose?
Accuracy
• How will you ensure the personal data is kept accurate and up to date?
Storage limitation
• Has a retention period been established for the personal data and can the system facilitate this (eg, deletion/anonymisation)?
Integrity and confidentiality (security)
• What technology is to be used?

• What are the security arrangements for the personal data?
• Where will the personal data being processed by the supplier be stored geographically?
• If the personal data is to be transferred/stored outside the UK/EEA, what additional arrangements are in place?
• Are there procedures for your employees to follow in relation to how to handle the personal data?
• Is any additional training required for your employees?
Accountability (including data subject rights)
• Have we included a data processor agreement in the contract with the system supplier?
• Is there functionality within the system to extract an individual's personal data in response to a subject rights request?

Risk assessment (to be completed by Data Protection Team in conjunction with project sponsor)

Likelihood of Harm				
	PROBABLE	**GREEN**	**RED**	**RED**
	POSSIBLE	**GREEN**	**AMBER**	**RED**
	REMOTE	**GREEN**	**GREEN**	**GREEN**
		MINIMAL	**SIGNIFICANT**	**SEVERE**
	Severity of Harm			

What does 'harm' mean?

It is something that has an impact on an individual and can affect their circumstances, behaviour, or choices.

For example, a significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

1 Risk to the individual whose data is being processed (e.g. privacy rights, identity theft, etc.)

Describe the source of the risk and nature of the potential impact to the individual(s).	What are you (or will you be) doing to ensure privacy and confidentiality rights are followed as much as possible?
Likelihood of harm to individuals (delete as appropriate):	Remote / Possible but unlikely / Probable (reasonable chance this will happen)
Severity of harm (delete as appropriate):	Minimal / Significant / Severe
Residual risk (delete as appropriate):	GREEN – AMBER – RED

2 Risk to the protection of the data (Security)

Describe the source of the risk and nature of the potential impact to the individual(s).	What are you (or will you be) doing to secure the data as much as possible?
Likelihood of harm to individuals (delete as appropriate):	Remote / Possible but unlikely / Probable (reasonable chance this will happen)
Severity of harm (delete as appropriate):	Minimal / Significant / Severe
Residual risk (delete as appropriate):	GREEN – AMBER – RED

DPO advice

DPO		Date:

Summary of DPO advice:

Review

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Sign off

Each data controller must keep a copy signed off by the Senior Manager responsible for the proposal, or equivalent, as evidence of due diligence.

Senior Manager	Add name and signature (electronic signature is acceptable)	Date:

EASTHALL PARK HOUSING COOPERATIVE - Employee Privacy Notice

EASTHALL PARK HOUSING COOPERATIVE as an employer is a data controller and collects and processes personal data and special category personal data relating its employees to manage the employment relationship it has with you as an employee and after you cease being an employee. We want to be transparent about how we collect and use your data and to meet our data protection obligations.

What personal information we collect and why is it processed?

We collect and process a range of information containing personal data about you. The table below details the personal data collected, the purpose for this and the legal basis for processing:

Personal Information	Purpose	Our legal basis
Basic personal information and contact details including: • Name • Address • date of birth • telephone number • emergency contact details	To maintain accurate employee records and contact details. To be able to contact someone in the event of an emergency. To allow contract, HR and business administration and defence against potential legal claims.	Necessary for the performance of a **contract** with you. Necessary for compliance with a **legal obligation**. Necessary for our **legitimate interests**
Recruitment records including: • CVs, interview notes and assessments • proof of right to work in UK (such as passports and visas) • evidence of education and qualifications • References • Employment Contract • Induction records	To make a decision about your suitability for the role you applied for. To comply with legislative and regulatory requirements To allow contract, HR and business administration and defence against potential legal claims.	Necessary for the performance of a **contract** with you Necessary for compliance with a **legal obligation**. Necessary for our **legitimate interests**
Payroll Information including: • pay and benefits entitlements • bank details • national insurance number	To pay employees and make appropriate tax payments and keep appropriate records. To allow HR and payroll and benefit administration and defence against potential legal claims.	Necessary for the performance of a **contract** with you Necessary for compliance with a l**egal obligation**

Work schedule and Leave including: • days of work • working hours • attendance • leave taken • leave requests • leave authorisation	To pay employees correctly To comply with legal requirements regarding working time To allow resource planning To manage statutory and non-statutory holiday and leave.	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation**. Necessary for our **legitimate interests**
Pension records including: • name • marital status • address • DOB • Salary • Pension age • Beneficiaries	To make appropriate pension payments. To comply with Legislative and regulatory requirements To allow pension administration and defence against potential legal claims. To allow auditing and reporting of Pension schemes	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Performance records including: • appraisal documents • probation and performance reviews • performance improvement plans • records of capability meetings and related correspondence/ warnings	To maintain a record of the operation of performance improvement processes. To allow HR administration and defence against potential legal claims.	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Disciplinary and grievance records including: • records of investigations • witness statements • notes of disciplinary or grievance meetings • correspondence with employees • relevant warnings	To maintain a record of the operation of disciplinary and grievance procedures and their outcome. To allow HR administration and defence against potential legal claims.	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Absence records including: • details of absence taken • reasons for absences • records of absence management discussions	To maintain records of the implementation of absence procedures To ensure that employees receive statutory and	Necessary for the performance of a **contract**

such as Return to Work Interviews • correspondence with employees	contractual sick pay or other pay entitlements and benefits To meet health and safety obligations and comply with the requirement to make reasonable adjustments To allow HR administration and defence against potential legal claims.	Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
CCTV Images	To maintain security of EASTHALL PARK HOUSING COOPERATIVE premises To provide a safe working environment for employees To comply with legislative and regulatory requirements	Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Information about Employee use of business equipment including: • access to computers • desk telephones • mobile phones • software and applications • Internet usage • Emails • Social media	To maintain the operation, security and integrity of business communications systems To provide IT and communications systems support To preventing excessive personal use	Necessary for compliance with a **legal obligation** Necessary for our **legitimate interests**
Photos and Videos	To promote the business of EASTHALL PARK HOUSING COOPERATIVE	Necessary for our **legitimate interests**

Special category personal information	**Purpose for processing**	**Our legal basis for processing**	**Special category legal basis**
Family leave including maternity, paternity, adoption and shared parental leave, parental leave and time off for dependents (which could include information about	To maintain a record of leave To ensure that employees receive statutory and contractual pay entitlements	Necessary for the performance of a **contract** Necessary for compliance with a **legal obligation**	Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the

Employee health and sexual orientation).		Necessary for our **legitimate interests**	field of employment.
Occupational Health records including: • medical records • health monitoring information • referrals for treatment such as counselling • reports and correspondence with external practitioners or GP's.	To assess suitability for work To meet Health & Safety obligations To comply with the requirements to provide reasonable adjustments	Necessary for compliance with a **legal obligation.** Necessary for our **legitimate interests**	Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment. Necessary for the purposes of preventative medicine or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health care systems.

We will collect this information in a variety of ways including directly from you, and from third parties as outlined below:

- Recruitment Agencies
- Former employers or other referees
- Occupational Health providers

Who we share your information with?

We will share your data as required by law to administer the working relationship that we have with you.

We may share your data with third parties, including third party service providers that process data on our behalf, in connection with payroll; the provision of employee benefits; the provision of occupational health services and IT services.

In relation to our third-party service providers, we have in place a written contract which only permits them to process your data for specified purposes and in accordance with our instructions. All their employees must be subject to a duty of confidentiality. The contract also requires third party service providers to take appropriate security measures in relation to your personal data which are in line with our policies. They are also not allowed to use your personal data for their own purposes.

How we secure your personal data?

We take the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

In addition, we limit the access that individuals have to your personal data to those who have a business need to know.

We have in place procedures to deal with any suspected data security breach and will notify you and the Information Commissioner's Office of a personal data breach when legally required to do so.

How long will we keep your personal data?

It is important that the personal data that we hold about you is accurate and current. Please keep HR advised of any changes to the personal data that is held, particularly contact details for you and your emergency contacts throughout the course of your employment.

We will hold your personal data for the duration of your employment and for as long as is necessary to fulfil the purposes of satisfying any legal, accounting or reporting requirements that we are subject to. The periods for which your data is held after the end of employment are set out in our Retention Policy.

In determining the retention period, we will consider the amount, nature and sensitivity of the personal data and the potential risk of harm from unauthorised use or disclosure; the purpose for which the data is being processed; and whether we can achieve those purposes through other means; and the applicable legal requirements for holding that data.

Your Rights

You have several rights in relation to your personal data. These are listed below. A fee will not generally be charged for exercising any of these rights unless your requests are manifestly excessive.

- The right to access information about the personal data we process about you and to obtain a copy of it;
- The right to require us to change incorrect or incomplete data;
- The right to require us to erase or stop processing your data; and

- The right to object to the processing of your data where we are relying on its legitimate interests as the legal ground for processing;

If you would like to exercise any of these rights, or if you have any concerns about how your personal data is being processed, please contact the FOI@easthallpark.org.uk

If you still believe that we have not complied with your rights, you can complain to the Information Commissioner's Office. Contact details are available at https://ico.org.uk/make-a-complaint/

What if you do not provide personal data?

You have some obligations under your employment contract to provide us with information. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith which you have as an employee. You may also have to provide us with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the information to us may mean that you are unable to exercise these statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable us to enter a contract of employment with you. If you do not provide other information, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Changes to this Privacy Notice

EASTHALL PARK HOUSING COOPERATIVE reserves the right to update this privacy notice at any time and will provide you with a new notice when making any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

Date of this version September 2022

Due for review September 2024

EASTHALL PARK HOUSING COOPERATIVE (Referred to as 'EASTHALL PARK HOUSING COOPERATIVE ') Privacy Notice for Clients

EASTHALL PARK HOUSING COOPERATIVE is a data controller and will collect and process your personal data. We are required to explain to all clients the personal data we collect, the purpose for processing and the legal basis we are relying on. This is an overview of our Privacy Notice, our full Privacy Notice is available on the EASTHALL PARK HOUSING COOPERATIVE website or you can request a copy from our Data Protection lead.

What personal information does EASTHALL PARK HOUSING COOPERATIVE collect and why is it processed?

EASTHALL PARK HOUSING COOPERATIVE collects and processes a range of information containing personal data about you. We process this information in order to be able to provide our services as a full service legal firm under our contract with you, or to comply with our legal obligations.

We are required to process your personal information when we have a contract with you for the provision of legal services and there may be some occasions where processing of special category personal data (such as health or ethnicity) is required. Where we process special category data it is necessary for the establishment, exercise or defence of legal claims

The personal data we collect, and use will only be the minimum necessary for your case. The following table shows the data we collect and process in relation to your legal case.

<table>
<tr><td>Data processed as necessary for the performance of a contract with you:

Contact Details (name, telephone numbers, email, address), for contacting you regarding the case we are dealing with.
Any personal data that is required to provide you with advice. This could be financial information; special category personal data or any other personal data as is required.

Payment details (bank account/ credit/debit card number), for processing payments required</td><td>Data Processed as necessary to meet a legal obligation:

Identification Documents (copies of passports, driving licence (photographic evidence and home address), for verifying your identification and your home address to comply with anti-money laundering obligations with which EASTHALL PARK HOUSING COOPERATIVE must comply.</td></tr>
<tr><td colspan="2">Data processed that is necessary for the legitimate interests of EASTHALL PARK HOUSING COOPERATIVE or a third party:

Contact Details (name and email), for keeping in touch and to send you information about our services, legal updates and information about our events. You will always be given the option to unsubscribe from receiving these emails and if you do not want to receive this information from EASTHALL PARK HOUSING COOPERATIVE then please email foi@easthallpark.org.uk</td></tr>
</table>

Who has access to your data?

Your information may be shared internally within EASTHALL PARK HOUSING COOPERATIVE on a need to know basis as appropriate. We may share your personal data with the following third parties where it is necessary for the legal service we provide to you:

- Other solicitors instructed by another party in any dispute or claim in which you are involved; your GP or expert witness instructed; any representative appointed to act on your behalf and to solicitors instructed to act as local agents on our behalf
- Service providers and their sub-contractors we are using to run our business including EASTHALL PARK HOUSING COOPERATIVE -for Identity checks; IT services providers; confidential waste disposal services and document storage providers; marketing service providers. Where we use these providers, we have appropriate contractual arrangements in place to ensure that these third parties do not use our data for their own purposes, will treat it with confidence and that they keep the data secure
- We will also share your data as required by law with, for example, Government authorities, law enforcement bodies, regulators for compliance with legal requirements.

How does EASTHALL PARK HOUSING COOPERATIVE protect your personal data?

EASTHALL PARK HOUSING COOPERATIVE takes the security of your data seriously. EASTHALL PARK HOUSING COOPERATIVE has policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by authorised persons who have a need to know in order to perform their duties and are under a duty to maintain the confidentiality and security of such information.

If personal data is transferred outwith the EU we will ensure that adequate safeguards are in place, relying on an adequacy agreement or other contractual terms as appropriate.

How long do we keep your personal data?

Once the case is complete and our legal services have ended, we will hold onto the personal data in your file for at least twenty years in line with the long prescriptive period for making legal claims.

Your rights

As a data subject, you have a number of rights in relation to your personal data. These are listed below.

- The right to access information about your personal data EASTHALL PARK HOUSING COOPERATIVE is processing and to obtain a copy of it;
- The right to require EASTHALL PARK HOUSING COOPERATIVE to change incorrect or incomplete data;
- The right to require EASTHALL PARK HOUSING COOPERATIVE to erase or stop processing your data in certain circumstances; and
- The right to object to the processing of your data where EASTHALL PARK HOUSING COOPERATIVE is relying on its legitimate interests as the legal ground for processing.

A fee will not generally be charged for exercising any of these rights unless your requests are unfounded or are manifestly excessive.

If you would like to exercise any of these rights, or if you have any concerns about how your personal data is being processed, please contact our Data Protection Lead at EASTHALL PARK HOUSING COOPERATIVE at foi@easthallpark.org.uk; or our Data Protection Officer at: info@rgdp.co.uk ; Telephone: 0131 222 3239.

If you still believe that EASTHALL PARK HOUSING COOPERATIVE has not handled your personal data properly or has not complied with your rights, you can complain to the Information Commissioner. Contact details are available at www.ico.org.uk/make-a-complaint/.

We may need to amend this Privacy Notice from time to time and we will notify you of any significant changes that we make.

Date of this version September 2022
Due for review September 2024

Privacy Policy

This website is operated by Easthall Park Housing Co-operative.
We at Easthall Park HC take your privacy seriously and we ask that you read this summary policy statement carefully, as it contains important information on:

- the personal information we collect about you;
- what we do with your personal information; and
- who your personal information might be shared with.

We are the controller of the personal information that we collect from you on our website, which means that we are legally responsible for how we collect, hold and use your personal information. It also means that we are required to comply with data protection laws when collecting, holding and using your personal information.
We have appointed a Data Protection Officer (RGDP) who ensures that we comply with data protection law. If you have any questions about this policy or how we hold or use your personal information, please contact them by e-mail info@rgdp.co.uk or[TK1] write to: Easthall Park Housing Co-operative, Glenburn Centre, 6 Glenburnie Place, Easthall, Glasgow, G34 9AN.
You can also contact us by: e-mail at FOI@easthallpark.org.uk

Your attention is particularly drawn to section 2 of this policy, which confirms that you consent to your personal information and sensitive personal information being held and used by us as described in section 1 of this policy.
Download a Full Copy of our Data Protection Policy from the website at www.easthallpark.org.uk

1. What personal information do we collect about you and why?

Our website is a place for you to find out more about us, your neighbourhood and the services available to you.
When you visit our website, we collect personal information about you when you:

- report a repair to us;
- make a complaint to us;
- download or submit a housing application form to us;
- complete and submit a “contact us” form to us;

We use such personal information to:

- provide you with the services that you have requested from us;
- communicate with you, including in response to any of your enquiries;
- improve our services and respond to changing needs;

- carry out repairs to your property;
- handle and resolve complaints made by / against you;
- keep the personal information that we hold about you accurate and up-to-date (if you provide any new personal information to us via the website); and

We may not be able to provide the above services to you if you do not provide us with sufficient personal information to allow us to do so.
We may also collect information about you via cookie files. A cookie is a small text file that is placed on to your computer or other access device when you visit our website. We may use cookie files for analytics purposes to gather statistical information on your use of our website.
The information we obtain from our use of cookies will not usually contain your personal information. Although we may obtain information about your computer or other access device, such as your IP address, your browser and / or other internet log information, this will not usually identify you personally.
If you do not want to accept cookies, you can change your browser settings so that cookies are not accepted. If you do this, please be aware that you may lose some of the functionality of this website.

2. What is our legal basis for holding and using your personal information?

Data protection laws require us to have a legal reason for collecting, holding and using your personal information.
In some circumstances, we may rely on your consent as the legal reason. By providing us with your personal information and sensitive personal information (relating to your health, racial or ethnic origin, religious or other beliefs or sexual orientation) and the personal information and sensitive personal information of other members of your household via our website, you:

- consent to it being used by us as described in section 1 of this policy; and
- confirm that you have informed the other members of your household over the age of 12 years old of the content of this policy and they have provided their consent to their personal information and sensitive personal information being used by us as described in section 1 of this policy.

You and the other members of your household have the right to withdraw your consent to us holding and using your and their personal information and sensitive personal information by contacting us. Once you / they have withdrawn your / their consent, we will no longer use your / their personal information and sensitive personal information for the purpose(s) set out in section 1 of this policy, which you originally agreed to, unless we have another legal reason for doing so.
Other legal reasons for holding and using your personal information are:

- performance and management of the tenancy agreement between us;

- legal and regulatory obligations which apply to us as a Registered Social Landlord or a Property Factor;
- protection of your vital interests; and
- our legitimate interests – while you have a legitimate interest in the protection of your personal information, we also have an overriding legitimate interest in handling and using your personal information, including sharing it with our service providers (listed in section 3 of this policy), for the purposes described in section 1 of this policy.

3. Who do we share your personal information with?

We may share your personal information with the following organisations for the purposes described in section 1 of this policy:

- our contractors to undertake repairs, works and maintenance;
- organisations providing benefits advice and support; and
- Police Scotland and the local authority anti-social behaviour department in relation to complaints involving anti-social or other criminal behaviour.

4. How long do we keep your personal information?

We will only keep your personal information for as long as we need to for the purposes described in section 1 of this policy, including to meet any legal, accounting, reporting or regulatory requirements. More information is contained in our data retention policy, which is available by contacting us.

5. How do we keep your personal information secure?

The security of your personal information is of paramount importance to us and we use technical and organisational measures to safeguard your personal information.
However, while we will use reasonable efforts to safeguard your personal information, the use of the Internet is not entirely secure and, for this reason, we cannot guarantee the security of any personal information that is transferred by or to you via the Internet. If you have any concerns about the security of your personal information, please contact us for more information.

6. What if you provide us with personal information about somebody else?

We understand that there may be situations where you provide us with personal information about somebody else. In those situations, you confirm that:

- the other individual has consented to you acting for them and to your use of their personal information;

- you have informed the other individual of our identity and the contents of this policy, including the purposes for which we will use that individual's personal information described in section 1 of this policy; and
- the other individual has explicitly consented to our use of that individual's personal information for the purposes described in section 1 of this policy.

This policy will apply to our collection, handling and use of the other individual's personal information in the same manner that it applies to your own personal information.

7. What rights do you have in relation to your personal information that we collect, hold and use?

It is important that the personal information that we collect, hold and use about you is accurate and current. Please keep us informed of any changes by contacting us. Under certain circumstances, the law gives you the right to request:

- A copy of your personal information and to check that we are holding and using it in accordance with legal requirements.
- Correction of any incomplete or inaccurate personal information that we hold and use about you.
- Deletion of your personal information where there is no good reason for us continuing to hold and use it. You also have the right to ask us to do this where you object to us holding and using your personal information (details below).
- Temporarily suspend the use of your personal information, for example, if you want us to check that it is correct or the reason for processing it.
- The transfer of your personal information to another organisation.
- You can also object to us holding and using your personal information where our legal basis is a legitimate interest (either our legitimate interests or those of a third party).

Please contact us if you wish to make any of the above requests. When you make a request, we may ask you for specific information to help us confirm your identity for security reasons. You will not need to pay a fee when you make any of the above requests, but we may charge a reasonable fee or refuse to comply if your request for access is clearly unfounded or excessive.

8. Feedback and complaints

We welcome your feedback on how we hold and use your personal information, and this can be sent to us.
You have the right to make a complaint to the Information Commissioner, the UK regulator for data protection, about how we hold and use your personal information. The Information Commissioner's website is https://ico.org.uk/ and complaints can be made here. If you would like to receive this policy in alternative format, for example, audio, large print or braille, please contact us.

9. Updates to this policy

We may update this policy at any time, and you should check this policy occasionally to ensure you are aware of the most recent version that will apply each time you access our website.

This version September 2022
Review due September 2024

EASTHALL PARK

Social Media Policy

Reviewed and approved by Committee	**2022 September**
Next review	**2024 September**

Table of Contents

Social Media Policy

1. Introduction

Effective use of social media can bring significant and measurable benefits to Easthall Park Housing Cooperative and its customers. These include opportunities to promote success stories, develop reach within the community and social housing sector, improve customer engagement and attract high quality staff and applicants.

Social media channels can spread Easthall Park Housing Cooperative s' messages quickly and to a range of audiences at little or no cost in order to supplement the Easthall Park Housing Cooperative s channel shift program and, unlike other traditional media channels, they can provide instant feedback from customers.

Along with these benefits come the risks inherent in managing something that is dynamic and unlimited in scale. These include the risk of reputational damage arising from misuse by staff or third parties, threats to the security of sensitive or confidential information, exposure to malware and a negative impact on productivity.

2. Purpose

This Social Media Policy aims to mitigate the risks associated with employees' use of social media. It provides all Easthall Park Housing Cooperative employees with a clear articulation of the expectations around the use of social media.

3. Scope

This policy has been produced for all Easthall Park Housing Cooperative employees including those involved in Easthall Park Housing Cooperative led projects.

4. Equality Analysis

There is potential for social media channels to be used for bullying and harassment of individuals. It is therefore important that the policy is

considered alongside staff conduct guidelines. Employee development will include reference to this policy in induction and management training.

5. Definitions

According to the Chartered Institute of Public Relations (CIPR), social media are: “Internet and mobile-based channels and tools that allow users to interact with each other and share opinions and content. It involves the building of communities or networks and encouraging participation and engagement.” This is the recognised definition for the purpose of this document.

This policy refers to three different types of social media account:-

- Professional Easthall Park Housing Cooperative Housing Account – used by representatives of Easthall Park Housing Cooperative to communicate messages from a departmental or corporate perspective; managed by a Departmental Social Media Champion
- Professional Personal Account – used by an individual member of staff, who is identifiable as an employee of Easthall Park Housing Cooperative through the content of their posts or their profile’s biographical information.
- Private Personal Account – used by an individual primarily for non-work activity.

Social networks covered by this policy include, but are not limited to, Facebook, Twitter, LinkedIn, YouTube, Instagram, Pinterest, Google+ and Tumblr.

6. Legislative Context

- UK GDPR and Data Protection Act 2018 and accompanying guidance in the Information Commissioner's Employment Practices Data Protection Code.
- Human Rights Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699).
- Copyright, Designs and Patents Act 1988

7. Health & Safety Implications

There is potential for social media channels to be used to cause emotional harm or mental distress to others. By producing this policy Easthall Park Housing Cooperative hopes to minimise any distress to its staff caused by the misuse of social media.

8. Policy and Principles

Easthall Park Housing Cooperative employees using social media in a professional capacity, either through a Professional Easthall Park Housing Cooperative account or a Professional Personal Account, should make sure that their communications do not do any of the following:-

- Bring Easthall Park Housing Cooperative into disrepute. For example, by making defamatory comments about individuals, other organisations or groups, or Easthall Park Housing Cooperative ; or posting images that are inappropriate, links to inappropriate content or using inappropriate language.
- Breach confidentiality. For example, revealing confidential information owned by Easthall Park Housing Cooperative relating to its activities, finances, people, or business plans, or the personal data of any individual who has not given informed consent (in writing) for their data to be published.
- Breach copyright. For example, using someone else's image or written content without their permission; failing to give acknowledgement where permission to reproduce something has been obtained
- Do anything that may be considered discriminatory against, or bullying and harassment of, any individual. For example, making offensive or derogatory comments relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive or linking to such content.
- Breach the terms of service of the social network. Each social network has different terms of use and community guidelines, which must be followed.

Employees using social media in a professional capacity should use the same safeguards that they would with any other form of communication about Easthall Park Housing Cooperative in the public sphere. These safeguards may include (but are not limited to):-

- ensuring that the communication has a purpose and benefit to Easthall Park Housing Cooperative
- obtaining a manager's permission before starting a public social media campaign
- checking the appropriateness of the content before it is published
- seeking advice if you are unsure of your objectives or required outcomes.

There should be a clear reason or reasons to set up a Professional Easthall Park Housing Cooperative Account and processes put in place to ensure that it is monitored and updated regularly during business hours.

Effective use of social media can enhance the reputation of Easthall Park Housing Cooperative and inform its customer base of forthcoming events and relevant information. Examples of good practise in the use of social media include but are not limited to:-

- Liking or forwarding a partner organisations post which may be deemed relevant to our customer base
- Providing information on events within Easthall Park Housing Cooperative 's areas of operation
- Providing information on adverse weather, outages, road closures etc within Easthall Park Housing Cooperative 's areas of operation
- Updating customer base on office closures for public holidays, training etc
- Raising awareness of services being offered by Easthall Park Housing Cooperative and projects Easthall Park Housing Cooperative is undertaking.

If you are in any doubt as to whether any form of content is relevant for Easthall Park Housing Cooperative 's corporate social media please consult with your manager.

A corporate services based social media champion will be responsible for:-

- ensuring that the account meets brand guidelines
- making sure that the login details are shared only with those who have a real need to use the account
- revoking access to the account where necessary, such as if an employee leaves the organisation
- ensuring that all content produced for the account is in line with this policy
- ensuring that the account is used regularly
- reporting any incidents where the administrator feels that an employee has misused the social media account.

Employees managing a Easthall Park Housing Cooperative account are expected to remove any comments that fit into the categories outlined under professional use of social media. Additionally, users should also remove comments that are:-

- spam, or trying to sell things
- fraudulent, deceptive or misleading
- in violation of any law or regulation.

Employees are encouraged to think carefully before removing users' comments, to ensure that users with good intentions do not feel that we are placing an unjustified restriction on their freedom of speech.

Social media users are encouraged to regularly check their accounts for messages and respond to any enquiries that they receive in a timely fashion within normal business hours.

Social media users who receive enquiries/approaches from media sources (newspapers, radio, TV) relating to their work at Easthall Park Housing Cooperative are encouraged to notify the departmental director or chief executive for guidance about how to respond (as they would if they received approaches from the media via any other channel).

9. Personal Use of Social Media

Easthall Park Housing Cooperative recognises that many employees will make use of social media in a personal capacity. Easthall Park Housing Cooperative employees using social media in a personal capacity should make sure that their communications do not do any of the following:-

- Bring Easthall Park Housing Cooperative into disrepute.
- Breach confidentiality.
- Breach copyright.
- Breach the terms of service of the social network
- Do anything that may be considered discriminatory against, or bullying and/or harassment of, any individual.

Misuse as outlined above may be regarded as a disciplinary offence.

Employees who openly disclose that they work for Easthall Park Housing Cooperative should include on their profile a statement or disclaimer explaining that the views expressed are theirs alone and that they do not necessarily reflect the views of Easthall Park Housing Cooperative Housing. However, if the content of a post is inappropriate, a disclaimer would not prevent disciplinary action.

To avoid confusion, Easthall Park Housing Cooperative prohibits the use of its logo(s) on social media when used for non-business reasons.

Employees are encouraged to familiarise themselves with privacy settings for each social media platform and choose a privacy level that they consider to be appropriate.

Employees are permitted to make reasonable and appropriate use of personal social media from Easthall Park Housing Cooperative 's computers or mobile devices, provided that this usage is limited to official rest breaks.

10. Procedures

Where it is found that an employee has misused social media, it may be regarded as a disciplinary offence in accordance with organisational disciplinary procedures. Although not exhaustive there are examples of misuse outlined earlier in this document.

Easthall Park Housing Cooperative reserves the right to monitor employees' internet usage in line with the ICT Acceptable Use Policy and the Communications Policy. In line with this, it may instigate an investigation into an employee's internet usage where there are suspicions that the employee has been using social media excessively for personal use when they should be working, or in a way that is in

breach of the rules set out in these policies. Authorisation to instigate an investigation into an employee's internet use can only be done by either the Director of Finance and Corporate Services or the Chief Executive, following consideration of a valid case for this from the individual's line manager.

Easthall Park Housing Cooperative monitors mentions of its brand name and associated terms in order to identify any risks to reputation and to gather customer feedback. Only content that is available in the public domain is subject to monitoring. Data monitored is processed anonymously for analysis purposes and is not held by Easthall Park Housing Cooperative . Easthall Park Housing Cooperative employees are advised to read the privacy guidance provided in this document.

This version September 2022
Due for review September 2024

Working from home or remotely away from the office - Data Protection considerations

Since the start of the Coronavirus pandemic, many people have been working remotely from home instead of their usual place of work. Even as the effects of the pandemic reduce, it seems clear that working from home will continue as new ways of working are adopted. Whether working from an office or remotely from home, data protection laws need to be complied with.

The following guidelines should be followed in all situations where staff are working from home or away from the office.

PURPOSE OF THIS DOCUMENT

This document sets out acceptable policy for compliance with Data Protection Act 2018 and the UK GDPR for users for accessing, viewing, modifying and deleting Easthall Park Housing Cooperative data (ie, processing personal data) and accessing its systems whilst away from the office, ie, in remote offices or your home.

DEFINITIONS

Data Protection Law means the UK General Data Protection Regulation; the UK Data Protection Act 2018; the EU Directive 2002/58/EC on privacy and electronic communications (PECR) as is applicable in the UK; and any laws replacing, amending or supplementing the same and any other applicable data protection or privacy laws.

Remote equipment / Home Worker refers to users using either company provided or your own device or systems or applications, to access and store company information, at your home or remotely, typically connecting to Easthall Park Housing Cooperative ’s Wireless Service or VPN (whichever is relevant).

Data Controller - The Data Controller is a person, group or organisation that alone or jointly with others determines the purposes and means of the processing of personal data. Easthall Park Housing Cooperative is the Data Controller for its employees’ personal data and [add example of other personal data, eg, tenants] (as applicable).

User – A member of staff, employee, contractor, visitor, or another person authorised to access and use Easthall Park Housing Cooperative ’s systems.

Data Processor – a person, group or organisation that processes personal data on the instructions of a Data Controller set out in a written contract.

POLICY INTRODUCTION

This policy covers the use of electronic devices which could be used to access Easthall Park Housing Cooperative ’s systems and store information, alongside employees’ own personal data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies.

Easthall Park Housing Cooperative , as the Data Controller, remains in control of the data regardless of the ownership of the device, or the location in which the data is processed. As an employee of Easthall Park Housing Cooperative you are required to keep any company information and data securely and comply with Data Protection law. You are required to assist and support Easthall Park Housing Cooperative in carrying out its legal and operational obligations, including co-operating with the IT team should it be necessary to access or inspect company data stored on your personal device or equipment at your home.

Easthall Park Housing Cooperative reserves the right to refuse, prevent or withdraw access or permissions for users to work from their homes and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its employees, business, reputation, systems or infrastructure.

Data Protection, Security and Confidentiality of Materials

You must follow Easthall Park Housing Cooperative 's policies and procedures in relation to working with personal data as if you were still based in the office. However, there are additional risks relating to working remotely. You should keep the following in mind:

a) The data protection principles still apply and need to be adhered to, ie, you should only access personal data that is needed for "specified, explicit and legitimate purposes". You should "limit what you take home to only what is necessary" and keep it there for "no longer than is necessary". You must consider "appropriate security", both at home and in transit. Additionally, if required to, you must be able to provide Easthall Park Housing Cooperative with evidence you are complying with these principles.

b) Never leave a computer with personal data on screen. An unauthorised person reading personal data is a data breach.

c) Never leave your computer 'logged on' when unattended. Think about who may access the device when you are not around – whether deliberate or accidental.

d) Ensure that rooms containing computers and other equipment, are secure when unattended, with windows closed and locked and blinds or curtains closed.

e) If making a phone or online conference call remember that it is confidential and consider who is around who might overhear.

f) Levels of Home Security should be at the same level as at work.

g) You should only work within Easthall Park Housing Cooperative 's approved systems, eg, Microsoft Office 365, Teams etc.

h) Do not hold person identifiable information on electronic devices. If you must download a document to your personal device, ensure it is deleted as soon as possible.

i) If using your own device, check for automatic uploads to Cloud storage systems. For example, if you have subscribed to iCloud or Dropbox, you may inadvertently be uploading Easthall Park Housing Cooperative 's documents to your personal account in these applications. You should disable these uploads whilst you are doing Easthall Park Housing Cooperative work.

j) Any paper taken from the office to work at home must be protected in transit and in your home.

k) Paper files should be 'signed out' from the office and 'signed in' again when returned.

l) Ensure paper is transported safely – in a wallet or case

m) Keep paperwork secure at home and out of sight of members of your family and others.

Loss or Theft

In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to Easthall Park Housing Cooperative 's IT department, in order that they can assist you to change the password to all company services and report this as a data breach if appropriate. (You must also cooperate with the IT Department in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.)

Easthall Park Housing Cooperative will not monitor the content of your personal devices, however the IT Department reserves the right to monitor and log data traffic transferred between your device and company systems.

In exceptional circumstances, for instance where Easthall Park Housing Cooperative requires access in order to comply with its legal obligations (e.g. obliged to do so by a Court of law or other law enforcement authority such as the Information Commissioner) Easthall Park Housing Cooperative will require access to company data and information stored on your personal device. Under these circumstances, all reasonable efforts will be made to ensure that Easthall Park Housing Cooperative does not access your private information.

Approval for Working Remotely

Line Managers will consider requests for home working in consultation with individual members of staff and may wish to confirm such arrangements with their senior manager and a Human Resources manager.

Compliance and Disciplinary Matters

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under Easthall Park Housing Cooperative 's disciplinary policy.

Date of this version September 2022
Due for review September 2024

Easthall Park Housing Cooperative

CCTV POLICY

1.Introduction

1.1 EPHC owns and operates CCTV and other forms of surveillance systems at various premises, including server room in offices. We do this for the purpose of enhancing security where we consider there to be a potential threat to the health, safety and wellbeing of individuals and to assist in the prevention and detection of risk of crime or anti-social behaviour.

1.2 EPHC acknowledges the obligations it incurs in operating such systems and the rights and freedoms of those whose images may be captured. We are committed to operating them fairly and within the law at all times and in particular will comply with the requirements of the UK General Data Protection Regulations (the 'UK GDPR') and UK Data Protection Act 2018 (the 'DPA 2018'). In developing this document, EPHC has incorporated the standards and practices from the Information Commissioner's Office Code of Practice, 'In the picture: A data protection code of practice for surveillance cameras and personal information' as well as the Surveillance Camera Commissioner Code of Practice 'A guide to the 12 principles'

1.3 This policy governs EPHC approach to installing and operating CCTV and other forms of surveillance systems and handling the information obtained. It is underpinned by the following key principles:

- Know we what the system is used for and review of its use;
- That we have completed a Privacy Impact Assessment (PIA) and this is published on our website via the Publication Scheme. Systems will only be installed with due consideration to the privacy impacts of doing so;
- That we will ensure clear signage is in place, with a published point of contact to deal with queries and complaints;
- There is clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used, and staff are aware of their responsibilities for CCTV;
- Clear rules, policies and procedures are in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them;
- That we have a policy for keeping the CCTV images we hold, and we ensure they are deleted once they are no longer needed;
- That we have a clear process for who can access the images, and a policy on disclosure;
- That the system we use follows recognised operational and technical standards. Systems will be appropriately specified and professionally installed, having due regard to appropriate technical and legal advice and other relevant guidance;
- Systems will only be installed where there is a clear identified and documented need;

- Systems will only be installed with due consideration to all alternative options;
- Appropriate technical and organisational measures will be employed to ensure the security of our systems and personal data, including relevant controls to govern access to and use of images;
- Appropriate measures will be taken to provide clear and accessible privacy information to individuals whose personal data is processed by systems;
- That we are clear on when CCTV images will be produced for criminal justice purposes;
- This policy will be supplemented by procedures, which provide detailed operational guidance on the installation, operation, use and maintenance of our systems.

2. Decisions on Installing CCTV and Surveillance Systems

2.1 EPHC recognises that using CCTV and other surveillance systems can be privacy intrusive. As such it will not install systems as a routine response to incidents of a criminal or anti-social nature. Notwithstanding this, we acknowledge the potential value of these systems as both a deterrent and a means of detection and will consider all potential installations on a case-by-case basis. In doing so the aim will be to demonstrate that installation is a justified, proportionate and effective solution to an identified problem or risk.

2.2 The impact on people's right to privacy and the availability of alternative and less intrusive options will be a key consideration. To this end, all potential installations will be subject to a Data Protection Impact Assessment (DPIA). All DPIAs will be conducted, recorded and signed off in accordance with our DPIA procedures. These have been developed in accordance with Information Commissioner's Office (ICO) guidance and prescribe the approach to be followed in identifying and assessing data protection risks, and in consulting with those whose privacy is likely to be affected, where appropriate. EPHC Data Protection Officer will advise on and review DPIAs as required.

2.3 EPHC will maintain a register of DPIAs as a record of decision making, installation authorisation and review. In the interests of transparency, the register and individual DPIAs shall be made publicly available on request.

3. System Specification and Installation

3.1 EPHC will procure and site systems in accordance with an agreed standard specification, which reflects recommended practices and incorporates privacy by design features. Relevant criteria will include, but not be limited to:

- Ensuring personal data can be easily located and extracted;
- Ensuring images are of an appropriate quality, relevant to their purpose;
- Ensuring that the date and time images are captured is easily identifiable;
- Ensuring that unnecessary images are not viewed or recorded;
- Ensuring that relevant retention periods can be complied with;

- Installing image only systems, which have no sound recording capability, as standard;
- Siting cameras to ensure only areas of interest are subject to surveillance and to minimise viewing areas not relevant to the purposes the system was installed for, with due regard given to planning permission requirements as necessary;
- Siting cameras to ensure they can produce quality images taking into account the environment where located;
- Siting cameras and equipment in secure locations, protected from unauthorised access and possible vandalism; and
- No cameras forming part of the system will be installed in a covert manner; and cameras which may be covered to protect them from weather or damage, would not be regarded as covert provided that appropriate signs are in place.

3.2 EPHC will engage the services of specialist contractors, in accordance with relevant procurement procedures, to advise on technical specifications and system configuration and design; and to carry out installation and maintenance. Such contractors will be required to demonstrate the appropriate credentials, expertise, and understanding of EPHC and data protection requirements.

3.3 EPHC will maintain a register of all system installations, detailing location and installation date, relevant technical specifications and system design features.

4.Access and Use of Images

4.1 Access to all equipment and images will be strictly controlled. Appropriate security measures will be in place to ensure entry to physical locations is limited to authorised personnel. As a general rule, such authorised personnel will be individuals appointed by EPHC specialist contractors, acting under explicit instruction. EPHC will have in place a written data processing agreement with these contractors which is UK GDPR compliant and clearly defines obligations, responsibilities and liabilities.

4.2 The specialist contractors will be responsible for setting and maintaining relevant technical security controls for each system, including passwords or access codes and for maintaining physical and digital access logs.

4.3 EPHC considers the following to be permitted reasons for monitoring:

- Prevention and detection of unacceptable behaviour, including aggressive or abusive actions, towards staff in EPHC premises;
- Prevention and detection of unauthorised access to, or other criminal activity within, EPHC premises; and/or
- General compliance with relevant legal obligations, regulatory requirements and EPHC policies and procedures.

4.4 EPHC shall not undertake routine monitoring of images captured in EPHC locations.

4.5 Access to images will be on an as required basis and in accordance with the purpose for which the system was installed. This will only be carried out where an incident has been reported that requires investigation or where there is clear suspicion that an incident has taken place. Where it is required to access or download recorded images in order to investigate an alleged incident a data request, authorised as a minimum by the relevant Manager, will be recorded in the CCTV Access Register.

4.6 Access to images may also be required in order to respond to a Subject Access Request (SAR). All requests for system footage by individuals will be treated as SARs and handled in line with EPHC SAR Procedures. In doing so EPHC acknowledges the requirement to balance the rights of data subjects against those of other individuals who appear in the requested images. On receipt of a SAR, arrangements will be made to retain, and prevent automatic deletion of, all images of the individual submitting the SAR that have been captured.

4.7 The general principle will be that requests for images will be authorised as a minimum by the relevant Manager at EPHC. Images will be supplied direct to the Manager that authorised the request, and receipt will be logged in the CCTV Access Register.

4.8 Disclosure of information from systems will be controlled and consistent with the purpose(s) for which the system was installed. As such disclosure is likely to be limited to law enforcement agencies or the EPHC legal advisers. The CCTV Access Register will contain relevant details of image disclosure, including named recipient and reason for disclosure. Any disclosure of images must be done by secure means.

4.9 EPHC will not routinely keep copies of images obtained through CCTV or other surveillance systems. Any images that are returned following disclosure will be disposed of securely in accordance with EPHC Data Retention and Destruction Policy and Procedures.

4.10 EPHC considers any attempted or actual misuse of CCTV or other surveillance systems or images by staff members to be a disciplinary matter, which will be handled in accordance with the relevant policy and procedures.

4.11 EPHC will consider requests from Police and other legal authorities when suitable reasons have been given and that are in line with their obligations under the Investigatory Powers Act 2016. Such disclosure of information must follow our disclosure procedure.

5. Reviewing Installations

5.1 As a minimum, each system will be reviewed 6 months after initial installation and every 12 months thereafter to ensure its continued use serves a legitimate purpose and is required; and that the installation specification and design is appropriate to this purpose. This will involve a

review and, as necessary, an update of the DPIA to reflect changes or actions required. EPHC have implemented review procedures

5.2 Where it is determined that a system is no longer needed, arrangements for decommissioning will be made promptly. This will involve removal of all cameras and associated equipment and signage in accordance with EPHC CCTV and surveillance system procedures.

5.3 Notwithstanding these regular reviews, EPHC will separately instruct its contractors to undertake periodic maintenance and security checks. Any works to repair or replace system components, or to amend system configuration or design will be carried out only under explicit instruction.

6. Privacy Information

6.1 EPHC shall be as transparent as possible in its usage of CCTV and surveillance systems and EPHC Privacy Notices will reference the collection of personal data via systems. Clear and prominent signage will also be in place where systems are in operation. Signage requirements will be included as part of the standard system specification, and the appointed specialist contractors will be required to confirm these have been met as part of the installation process. In accordance with good practice these will state the general purpose for which the system is being used and contain relevant contact details where any enquiries should be directed. In this regard, complaints about implementation of or compliance with this Policy or the associated procedures, will be handled in accordance with EPHC Complaints Handling Procedure.

6.2 EPHC acknowledges that individuals also have the right to complain to the Information Commissioner's Office (ICO) directly if they feel EPHC is not operating CCTV and surveillance systems in accordance with the UK GDPR and/or DPA 2018.

7.Review

This policy will be reviewed every two years or sooner if required by changes in legislation or regulatory guidance.

Dated	220922
Document Owner	Anila Ali
Approved By	Committee
Review Date	September 2024
Version	0.1

Data Processor Contract Addendum

between

(1) [Insert Name of **Customer**] (the Customer, hereinafter referred to as **"Data Controller"**)

and

(2) [Insert Name of **Supplier**] (the Supplier, hereinafter referred to as "**Data Processor**").

WHEREAS the Data Controller processes Personal Data in connection with its business activities; and whereas the Data Controller has engaged the services of the Data Processor to process Personal Data on its behalf, the parties do hereby agree as follows:-

1. Definitions

1.1 The terms **"process/processing", "data subject", "Data Processor", "Data Controller", "personal data", "personal data breach"**, and **"data protection impact assessment"** shall have the same meaning as described in Data Protection Laws;

1.2 "**Addendum**" means this Data Processor Contract Addendum;

1.3 "**Authorised Sub-Data Processors**" means (a) those Sub-Processors (if any) set out in Schedule 2 (*Authorised Sub-Processors*); and (b) any additional Sub-Processors consented to in writing by the Data Controller in accordance with section 5.1;

1.4 "**Data Protection Laws**" means, in relation to any Personal Data which is Processed in the performance of the Main Agreement, the UK General Data Protection Regulation ("UK GDPR"); the UK Data Protection Act 2018; the EU Directive 2002/58/EC on privacy and electronic communications, as transposed into UK legislation; and any applicable decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, the Information Commissioner's Office and other applicable UK government departments; in each case together with all laws implementing, replacing, amending or supplementing the same and any other applicable data protection or privacy laws;

1.6 "**Personal Data**" means the data described in Schedule 1 (*Details of Processing of Personal Data*) and any other personal data processed by the Data Processor on behalf of the Data Controller pursuant to or in connection with the Main Agreement;

1.7 "**Main Agreement**" means the services agreement into which this Addendum is incorporated;

1.8 "**Services**" means the services described in the Main Agreement;

1.9 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to Data Processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

1.10 "**Sub-Processor**" means any Data Processor (including any affiliate of the Data Processor) appointed by the Data Processor to process personal data on behalf of the Data Controller;

1.11 "**Supervisory Authority**" means (a) the UK Information Commissioner's Office pursuant to Article 51 of the UK GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

1.12 "**Customer**" means the Customer under the Main Agreement.

1.13 **"Supplier"** means the Supplier under the Main Agreement.

2. Processing of Personal Data

2.1 The parties agree that the Customer is a Data Controller and that the Supplier is a Data Processor for the purposes of processing Personal Data.

2.2 Each party shall at all times in relation to processing connected with the Main Agreement comply with Data Protection Laws.

2.3 The Data Processor shall only process the types of Personal Data relating to the categories of data subjects for the purposes of the Main Agreement and for the specific purposes in each case as set out in Schedule 1 (Details of Processing of Personal Data) to this Addendum and shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with the Data Controller's documented instructions (whether in the Main Agreement or otherwise) unless processing is required by applicable law to which the Data Processor is subject, in which case the Data Processor shall, to the extent permitted by such law, inform the Data Controller of that legal requirement before processing that Personal Data.

2.4 The Data Processor shall immediately inform the Data Controller, if in its opinion, an instruction pursuant to the Main Agreement or this Addendum infringes Data Protection Laws.

2.5 The Data Controller warrants to and undertakes with the Data Processor that all data subjects of the Personal Data have been or will be provided with appropriate privacy notices and information to establish and maintain for the relevant term the necessary legal grounds under Data Protection Laws for transferring the Personal Data to the Data Processor to enable the Data Processor to process the Personal Data in accordance with this Addendum and the Main Agreement.

3. Data Processor Personnel

3.1 The Data Processor shall treat all Personal Data as strictly confidential and shall inform all its employees, agents, contractors and/or Authorised Sub- Processors engaged in processing the Personal Data of the confidential nature of such Personal Data.

3.2 The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent, contractor and/or Authorised Sub- Processor who may have access to the Personal Data, ensuring in each case that access is limited to those persons or parties who need to access the relevant Personal Data, as necessary for the purposes set out in section 2.1 above in the context of that person's or party's duties to the Data Processor.

3.3 The Data Processor shall ensure that all such persons or parties involved in the processing of Personal Data are subject to:

3.3.1 confidentiality undertakings or are under an appropriate statutory obligation of confidentiality; and

3.3.2 user authentication processes when accessing the Personal Data.

4. Security

The Data Processor shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5. Sub-processing

5.1 Subject to section 5.4, the Data Processor shall not engage any Sub- Processor to process Personal Data other than with the prior specific or general written authorisation of the Data Controller.

5.2 In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Data Processors (Sub-Processors), thereby giving the Data Controller the opportunity to object to such changes.

5.3 With respect to each Sub- Processor, the Data Processor shall:

5.3.1 carry out adequate due diligence on each Sub- Processor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Addendum including without limitation, sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of Data Protection Laws and this Addendum;

5.3.2 include terms in the contract between the Data Processor and each Sub-Processor which are the same as those set out in this Addendum, and shall supervise compliance thereof;

5.3.3 insofar as that contract involves the transfer of Personal Data outside of the UK, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Data Controller into the contract between the Data Processor and each Sub- Processor to ensure the adequate protection of the transferred Personal Data, or such other arrangement as the Data Controller may approve, as providing an adequate protection in respect of the processing of Personal Data in such third country(ies); and

5.3.4 remain fully liable to the Data Controller for any failure by each Sub-Processor to fulfil its obligations in relation to the Processing of any Personal Data.

5.4 As at the date of the Main Agreement or (if later) implementation of this Addendum, the Data Controller hereby authorises the Data Processor to engage those Sub-Processors set out in Schedule 2 (*Authorised Sub- Processors*).

6. Data Subject Rights

6.1 The Data Processor shall without undue delay, and in any case within two (2) working days, notify the Data Controller if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in chapter 3 of the UK GDPR, and shall provide full details of that request.

6.2 The Data Processor shall co-operate as reasonably requested by the Data Controller to enable the Data Controller to comply with any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and to comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or the Main Agreement, which shall include:

6.2.1 the provision of all information reasonably requested by the Data Controller within any reasonable timescale specified by the Data Controller in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to a data subject;

6.2.2 where applicable, providing such assistance as is reasonably requested by the Data Controller to enable the Data Controller to comply with the relevant request within the timescales prescribed by Data Protection Laws; and

6.2.3 implementing any additional technical and organisational measures as may be reasonably required by the Data Controller to allow the Data Controller to respond effectively to relevant complaints, communications or requests.

7. Personal Data Breach Management

7.1 In the case of a personal data breach, the Data Processor shall, without undue delay, notify the personal data breach to the Data Controller providing the Data Controller with sufficient information which allows the Data Controller to meet any obligations to report a personal data breach under Data Protection Laws. Such notification shall as a minimum:

7.1.1 describe the nature of the personal data breach, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;

7.1.2 communicate the name and contact details of the Data Processor’s data protection officer or other relevant contact from whom more information may be obtained;

7.1.3 describe the likely consequences of the personal data breach; and

7.1.4 describe the measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.2 The Data Processor shall fully co-operate with the Data Controller and take such reasonable steps as are directed by the Data Controller to assist in the investigation, mitigation and remediation of each personal data breach, in order to enable the Data Controller to:

(i) perform a thorough investigation into the personal data breach; and

(ii) formulate a correct response and to take suitable further steps in respect of the personal data breach in order to meet any requirement under Data Protection Laws.

7.3 The parties agree to coordinate and cooperate in good faith on developing the content of any related public statements or any required notices for the affected persons. The Data Processor shall not inform any third party without first obtaining the Data Controller's prior written consent, unless notification is required by law to which the Data Processor is subject, in which case the Data Processor shall, to the extent permitted by such law, inform the Data Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Data Controller before notifying the personal data breach.

8. Data Protection Impact Assessments and Consultation

The Data Processor shall, at the Data Controller's request, provide reasonable assistance to the Data Controller with any data protection impact assessments and any consultations with any Supervisory Authority of the Data Controller as may be required in relation to the processing of Personal Data by the Data Processor on behalf of the Data Controller.

9. Deletion or Return of Data Controller Personal Data

The Data Processor shall promptly and in any event within 90 (ninety) calendar days of the earlier of:

(i) cessation of processing of Personal Data by the Data Processor; or

(ii) termination of the Main Agreement, at the choice of the Data Controller either return all Personal Data to the Data Controller or securely dispose of Personal Data (and thereafter promptly delete all existing copies of it)

except to the extent that any applicable law requires the Data Processor to store such Personal Data.

10. Audit Rights

10.1 The Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this Addendum and Data Protection Laws and allow for and contribute to audits, including inspections by the Data Controller or another auditor mandated by the Data Controller of any premises where the processing of Personal Data takes place.

10.2 The Data Processor shall permit the Data Controller or another auditor mandated by the Data Controller during normal working hours and on reasonable prior notice to inspect, audit and copy any relevant records, processes and systems in order that the Data Controller may satisfy itself that the provisions of Data Protection Laws and this Addendum are being complied with.

10.3 The Data Processor shall provide full co-operation to the Data Controller in respect of any such audit and shall at the request of the Data Controller, provide the Data Controller with evidence of compliance with its obligations under this Addendum and Data Protection Laws.

11. International Transfers of Data Controller Personal Data

11.1 The Data Processor shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Sub- Processor to (permanently or temporarily) process the Personal Data in a country outside of the UK without an adequate level of protection, other than in respect of those recipients in such countries listed in Schedule 3 (*Authorised Transfers of Personal Data*), unless authorised in writing by the Data Controller in advance.

11.2 When requested by the Data Controller, the Data Processor shall promptly enter into (or procure that any relevant Sub- Processor of the Data Processor enters into) an agreement with the Data Controller on Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Personal Data in a country outside of the UK without an adequate level of protection.

12. Liability

The disclaimers and limitations of liability set out under the Main Agreement shall apply also to this Addendum.

13. Miscellaneous

13.1 Any obligation imposed on the Data Processor under this Addendum in relation to the processing of Personal Data shall survive any termination or expiration of the Main Agreement.

13.2 With regard to the subject matter of this Addendum, in the event of any conflict or inconsistency between any provision of the Main Agreement and any provision of this Addendum, the provision of this Addendum shall prevail. In the event of any conflict or inconsistency between the Main Agreement or this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14. Signatories

This Agreement is signed on behalf of each of the parties by its duly authorised representative as follows:-

Data Controller

_____	_____
SIGNATURE	NAME
_____	_____
POSITION	DATE

Data Processor

SIGNATURE	NAME
POSITION	DATE

SCHEDULE 1: Details of Processing of Personal Data

This Schedule 1 includes certain details of the processing of Personal Data as required by Article 28(3) of the UK GDPR.

Subject matter and duration of the processing of Personal Data
[ENTER DETAILS]
The nature and purpose of the processing of Personal Data
[ENTER DETAILS]
The types of Personal Data to be processed
[ENTER DETAILS
The categories of data subject to whom the Personal Data relates
[ENTER DETAILS]

SCHEDULE 2: Authorised Sub- Processors

[ENTER DETAILS]

SCHEDULE 3: Authorised transfers of Data Controller personal data

[ENTER DETAILS]

Data Sharing Agreement

between

[insert name of Data Controller] ("**Party 1**")

and

[Insert organisation name] ("**Party 2**")

(each a "**Party**" and together the "**Parties**").

WHEREAS

(a) Party 1 and Party 2 intend that this data sharing agreement will form the basis of the data sharing arrangements between the parties (the "Agreement");

(b) The intention of the Parties is that they shall each be independent Data Controllers in respect of the Data that they process under this Agreement; and

(c) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of **[insert details of relationship/ contract with Party 2]**.

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

1.1 In construing this Agreement, capitalised words and expressions shall have the meaning set out below:

"Agreement"	means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;
"Business Day"	means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;
"Data"	means the information which contains Personal Data and Special Category Personal Data (both of which have the definition ascribed to them in Data Protection Law) described in Part 1;

"Data Controller" has the meaning set out in Data Protection Law;

"Data Protection Law" means the provisions of the Data Protection Act 2018, the UK General Data Protection Regulation ("UK GDPR"), the EU Directive 2002/58/EC on Privacy and Electronic Communications, as transposed into UK legislation, and any applicable decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, the Information Commissioner's Office and any other applicable UK government departments, in each together with all laws implementing, replacing, amending or supplementing the same and any other applicable data protection or privacy laws;

"Data Recipient" means the party (being either Party 1 or Party 2, as appropriate) to whom Data is disclosed;

"Data Subject" means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement as listed in Part 1;

"Data Subject Request" means a request to either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the data or the activities of the parties contemplated by this Agreement;

"Disclosing Party" means the party (being either Party 1 or Party 2, as appropriate) disclosing Data to the Data Recipient;

"Information Commissioner" means the UK Information Commissioner and any successor;

"Law" means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;

"Legal Basis" means in relation to either Party, the legal basis for sharing the Data as described in Clause 2 and as set out in Part 2;

"Purpose" means the purpose referred to in Part 2;

"Representatives" means, as the context requires, the representative of Party1 and/or the representative of Party 2 as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice in writing by the relevant Party to the other Party;

"Schedule" means the Schedule in 5 Parts annexed to this Agreement and a reference to a "Part" is to a Part of the Schedule; and

"Security Measures" has the meaning given to that term in Clause 2.4.6.

1.2 In this Agreement unless the context otherwise requires:

1.2.1 words and expressions defined in Data Protection Law shall have the same meanings in this Agreement so that, in the case of Data Protection Law, words and expressions shall be interpreted in accordance with:

(a) the UK General Data Protection Regulation; and

(b) the UK Data Protection Act 2018;

1.2.2 more generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions, consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder.

2 DATA SHARING

Purpose and Legal Basis

2.1 The Parties agree to share the Data as specified in Part 1 of the Schedule for the Purpose in accordance with the provisions of Part 2 of the Schedule.

2.2 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.

2.3 Each Party shall ensure that it processes the Data fairly and lawfully in accordance with Data Protection Law and each Party as Disclosing Party warrants to the other Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis.

Parties Relationship

2.4 The Parties agree that the relationship between them is such that any processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

2.4.1 it is a separate and independent Data Controller in respect of the Data that it processes under this Agreement, and that the Parties are not joint Data Controllers or Data Controllers in common;

2.4.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

2.4.3 it shall comply with its obligations under Part 5 of the Schedule;

2.4.4 it shall not transfer any of the Data outside the United Kingdom and / or the European Economic Area except to the extent agreed by the Disclosing Party;

2.4.5 Provided that where the Data has been transferred outside the United Kingdom and / or the European Economic Area, the Disclosing Party may require that the Data is transferred back to within the United Kingdom and / or the European Economic Area:

(a) on giving not less than 3 months' notice in writing to that effect; or

(b) at any time in the event of a change in Law which makes it unlawful for the Data to be processed in the jurisdiction outside the United Kingdom and / or the European Economic Area where it is being processed; and

2.4.6 it shall implement appropriate technical and organisational measures including the security measures set out in Part 5 of the Schedule (the "**Security Measures**"), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.

2.5 The Disclosing Party undertakes to notify in writing to the other as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient, to ensure that the Data Recipient is then able to correct its records. This will happen whether the error is discovered through existing Data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Disclosing Party by the Data Subjects themselves).

Transferring Data

2.6 Subject to the Data Recipient's compliance with the terms of this Agreement, the Disclosing Party undertakes to endeavour to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

3 BREACH NOTIFICATION

3.1 Each Party shall, promptly (and, in any event, no later than 12 hours after becoming aware of the breach or suspected breach) notify the other party in writing of any breach or suspected breach of any of that Party's obligations in terms of Clauses 1 and/or 2 and of any other unauthorised or unlawful processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):

3.1.1 the nature of the personal data breach or suspected breach;

3.1.2 the date and time of occurrence;

3.1.3 the extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by the that party to contain the breach or suspected breach; and

3.1.4 any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.

3.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.

3.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in law.

4 DURATION, REVIEW AND AMENDMENT

4.1 This Agreement shall come into force immediately on being executed by all the Parties and continue for [***insert termination: this will be when Parties cease sharing data in terms of contractual relationship with each other***], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.

4.2 This Agreement will be reviewed one year after it comes into force and every two years thereafter until termination or expiry in accordance with its terms.

4.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:

4.3.1 the terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement; or

4.3.2 the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.

4.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.

4.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:

4.5.1 suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or

4.5.2 terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within five (5) Business Days of receiving written notice of the breach.

4.6 Where the Disclosing Party exercises its rights under Clause 4.5 it may request the return of the Data (in which case the Data Recipient shall, no later than fourteen (14) days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part and shall confirm having done so to the other Party in writing), save that the Data Recipient will be permitted to retain one copy for the purpose of complying with, and for so long as required by, any

law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.

5 LIABILITY

5.1 Nothing in this Agreement limits or excludes the liability of either Party for:

5.1.1 death or personal injury resulting from its negligence; or

5.1.2 any damage or liability incurred as a result of fraud by its personnel; or

5.1.3 any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.

5.2 The Data Recipient indemnifies the Disclosing Party against any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the other party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms of this Clause 5.2 is limited to £# (# STERLING) in the aggregate for the duration of this Agreement.

5.3 Subject to Clauses 5.1 and 5.2 above:

5.3.1 each Party excludes all liability for breach of any conditions implied by law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;

5.3.2 neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data provided to them by the other Party; and

5.3.3 use of the Data by both Parties is entirely at their own risk and each party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one party from offering clarification and guidance to the other party as to appropriate interpretation of the Data.

6 DISPUTE RESOLUTION

6.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

6.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.

6.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause 6.2, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

6.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause 8.

6.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

7 NOTICES

Any Notices to be provided in terms of this Agreement must be provided in writing and addressed to the relevant Party in accordance with the contact details noted in Part 4 of the Schedule, and will be deemed to have been received (i) if delivered personally, on the day of delivery; (ii) if sent by first class post or other next working day delivery, the second day after posting; (iii) if by courier, the date and time the courier's delivery receipt if signed; (iv) if by fax, the date and time of the fax receipt; or, if sent by email, the date of the sending of the email.

8 GOVERNING LAW

This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) (a **"Dispute"**) shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

IN WITNESS WHEREOF these presents consisting of this and the preceding 9 pages together with the Schedule in 5 parts hereto are executed by the Parties hereto as follows:

PARTY 1

_____ _____

SIGNATURE NAME

_____ _____
POSITION DATE

PARTY 2

_____ _____
SIGNATURE NAME

_____ _____
POSITION DATE

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN PARTY1 AND PARTY 2

SCHEDULE PART 1 – DATA[DM1]

DATA SUBJECTS

For the purposes of this Agreement, Data Subjects are all living persons about whom information is transferred between the Parties.

SCHEDULE PART 2: PURPOSE AND LEGAL BASIS FOR PROCESSING

Purpose[DM2]

The Parties are exchanging Data to allow

Legal Basis[DM3]

SCHEDULE PART 3 - DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of personal data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent that data is physically transported, the following media are used:

- Face to face[DM4]
- ~~Secure email~~
- Courier
- Encrypted removable media

~~The data is encrypted, with the following procedure(s):~~

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

Party 1

Name: #

Job Title: #

Address: #

E-mail: #

Telephone Number: #

Party 2

Name: #

Job Title: #

Address: #

E-mail: #

Telephone Number: #

SCHEDULE PART 5 – SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

2.1 Any use of data processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:
The unauthorised use of IT systems is prevented by:

- User ID[DM5]
- ~~Password assignment~~
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments

The following additional measures are taken to ensure the security of any Data:

3 Disposal of Assets

Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data must be physically destroyed or the information must be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

4 Malicious Software and Viruses

Each Party must ensure that:

4.1.1 PCs and other electronic devices used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

SCHEDULE PART 6 – DATA GOVERNANCE

Data accuracy

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any information, in excess of information reasonably required in order to allow both organisations to comply with their obligations, is shared, the Data Recipient will notify the other party immediately and arrange the secure return of the information and secure destruction of any copies of that information.

Data retention and deletion rules

The Parties shall independently determine what is appropriate in terms of their own requirements for data retention.

Both Parties acknowledge that Data that is no longer required by either organisation will be securely removed from its systems and any printed copies securely destroyed.

PARTY 1

_____
SIGNATURE

PARTY 2

_____
SIGNATURE

Template: Joint Data Controller Agreement

Notes on Joint Controllers under the UK GDPR

Article 26 of the UK GDPR states:

Joint controllers
1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

The Data Protection Act 2018, Section 58 states:

Joint controllers
(1) Where two or more competent authorities jointly determine the purposes and means of processing personal data, they are joint controllers for the purposes of this Part.
(2) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of an enactment.
(3) The arrangement must designate the controller which is to be the contact point for data subjects.

Notes:
To be a Joint controller both parties must be determining the purposes of processing. The ICO refers to solicitors; accountants and other professional advisers as falling into this category. The Controller may also have statutory obligations to share personal data with particular organisations.

- They must determine who is responsible for the various obligations that Controllers have under the GDPR in particular:
- Who will provide fair processing information to the data subjects;
    - Who will take the lead in dealing with data subject rights?
    - UK law may determine who has responsibilities – see above.
- You should designate which controller will be the contact point for data subjects.
- You should advise the data subject of the essence of the arrangement.

NB the data subject can still exercise their rights in relation to each controller no matter what arrangements you put in place.

JOINT DATA CONTROLLER AGREEMENT

between

(1) [ ] (the "**First Party**");

and

(2) [ ] (the "**Second Party**").

WHEREAS the First Party has procured the services of the Second Party and in the course of the provision of those services the Parties will share Information and act as Joint Data Controllers. Accordingly, the Parties wish to enter into an agreement to govern the terms of such Information sharing between them, and to set out their respective rights and obligations in relation thereto. [You may wish to put in more about the relationship between the parties here. This document is designed to cover the situation where data from the Controller is being shared with another party rather than data being shared though a common data base.]

NOW IT IS HEREBY AGREED AND DECLARED AS FOLLOWS:

1. Definitions and Interpretation

1.1 In this Agreement, the following words and expressions shall have the meanings ascribed to them in this clause 1.1:

"**Agreed Purposes**"	the agreed purposes set out in clause 2.2;
"Agreement"	means this Joint Data Controller Agreement;

“Data Controller” means the natural or legal person, public authority, agency or other body which, alone, or jointly with others, determines the purposes and means of the processing of personal data;

“Data Discloser” means the Party transferring Personal Data to the Data Receiver;

“Data Receiver” means the Party receiving Personal Data from the Data Discloser;

“**Data Subject”** means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

“Information” means all information, Personal Data, Special Category Data, non-personal data, documents or other material that is obtained from or in relation to a Data Subject pursuant to this Agreement;

“Data Protection Law” means the provisions of the Data Protection Act 2018, the UK General Data Protection Regulation (“UK GDPR”), the EU Directive 2002/58/EC on Privacy and Electronic Communications, as transposed into UK legislation, and any applicable decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, the Information Commissioner’s Office and any other applicable UK government departments, in each together with all laws implementing, replacing, amending or supplementing the same and any other applicable data protection or privacy laws;

“Party” means a party to this Agreement, and **“Parties”** means two or more of them;

"Personal Data" means any information relating to an identified or identifiable Data Subject, including, for the purposes of this Agreement, Special Category Data;

"Shared Personal Data" means the Personal Data and Special Category Data shared between the Parties in terms of this Agreement;

"Special Category Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and data relating to criminal convictions and offences; and

"Term" has the meaning ascribed to it in clause 12.1.

1.2 In this Agreement, unless the contrary intention appears;

1.2.1 the headings and captions in this Agreement are inserted for convenience only and shall be ignored in construing and interpreting this Agreement;

1.2.2 a reference in this Agreement to any clause or paragraph is respectively, except where it is expressly stated to the contrary, a reference to such clause or paragraph of this Agreement; and

1.2.3 references to any law shall, unless the context otherwise requires, be construed as including references to any subsequent law directly or indirectly amending, consolidating, extending, replacing or re-enacting the same, and will include any orders, regulations, instruments, or other subordinate legislation made under the relevant law.

2. Purpose

2.1 This Agreement sets out the framework for the sharing of Information between the Parties as Data Controllers and the procedures that the Parties shall follow and the responsibilities of each of the Parties.

2.2 The Parties shall only process Personal Data for the following agreed purposes ("Agreed Purposes") and shall not process Shared Personal Data for any other purpose:-

- [Insert purposes particular to agreement or statutory provision]

2.3 For the purposes of this Agreement, the following types of Personal Data (Shared Personal Data) may be shared between the Parties during the Term of this Agreement:-

- [Insert Shared Personal Data particular to agreement or statutory provision]

3. Identity of Data Controller

Each Party shall be a Joint controller with the other Party in relation to the Shared Personal Data.

4. Compliance with Data Protection Laws

4.1 Each Party shall ensure compliance with Data Protection Law at all times during the Term of this Agreement.

4.2 Each Party shall ensure that it processes Personal Data only on the basis of one of the legal grounds permitted by Data Protection Law.

5. Security of Information

Each Party shall ensure that it has implemented the appropriate technical and organisational security measures needed to ensure that its processing of Personal Data complies with this Agreement, and with Data Protection Law.

6. Transfer and Processors

6.1 Neither party shall share or transfer Shared Personal Data in a way that is incompatible with the purpose of sharing as set out in this agreement and that it is carried out in a fair, lawful and transparent manner, in accordance with Data Protection Law.

6.2 If a Party uses a processor to process any Information or Shared Personal Data obtained under this Agreement, subject to clause 6.1, it shall ensure that it has in place a legally binding agreement with the processor to govern such processing. Such agreement must provide that the processor will carry out its processing activities in a manner that does not cause either Party to be in breach of its obligations under applicable Data Protection Law.

6.3 Both Parties shall, subject to clause 6.1, ensure that they do not transfer any Information or Shared Personal Data outside the European Economic Area or to an international organisation unless such transfer is permitted by Data Protection Law and provisions which are adequate and equivalent to the terms of this Agreement are in place in respect of the transfer of the Shared Personal Data.

7. Information to be Provided to Data Subjects

7.1 The Data Discloser shall be responsible for providing the Data Subject with all information required by Data Protection Law to be provided to the Data Subject at the point of collection of that Personal Data. The Data Discloser will therefore be the point of contact for Data Subjects.

7.2 Both Parties shall, in respect of Shared Personal Data, ensure that their privacy notices are clear and provide sufficient information to the Data Subject in order for them to understand what personal data is collected, how it is processed, the purpose for which it is processed, when and why their personal data may be shared, to whom personal data may be transferred and their rights under applicable Data Protection Law.

7.3 It shall be the responsibility of the Party receiving a Subject Access Request (SAR) or any other request from a data Subject to exercise his or her rights under Data Protection Law to comply with it in respect of the Shared Personal Data held by that Party. The Party who received the SAR will seek the views of the other Party in relation to disclosure of information under a SAR within 7 calendar days of receiving a SAR.

7.4 Each Party shall keep a record of Data Subject Requests received by that Party and any information that was provided to the Data Subject and/or exchanged with the other Party. The Parties agree to provide such reasonable assistance to the Party receiving a Data Subject Request (within 7 calendar days of any written request for same) as is necessary for the receiving Party to comply with the Request.

8. Accuracy, Retention and Storage

8.1 The Data Discloser shall ensure that the Shared Personal Data is up to date and accurate at the point at which it is disclosed to the Data Receiver. Where either party becomes aware that any Shared Personal Data is not accurate or up to date, that Party shall inform the other and that Party shall take steps to ensure that the Shared Personal Data is updated and/or rectified as appropriate.

8.2 The Parties shall not retain or process the Shared Personal Data for longer than is necessary to carry out the Agreed Purposes or in order to comply with any statutory, professional or other legal requirements.

8.3 On termination of this Agreement for any reason, the Data Receiver shall promptly (and in any event within 5 working days of termination) ensure that all Shared Personal Data held by it is permanently and securely destroyed so that it is no longer retrievable [*and/or deliver to the Data Discloser all Shared Personal Data disclosed by the Data Discloser together with all copies in any form and in any media in the Data Receiver's power, possession or control*]. The Data Receiver shall provide such information as is necessary to enable the Data Discloser to satisfy itself of the Data Receiver's compliance with this clause.

9. Complaints and Breaches

9.1 The Parties to this Agreement are responsible for ensuring that their staff, including, but not limited to officers, employees, volunteers, directors, trustees and board members, are bound by this Agreement and adhere to its terms. The Parties are individually responsible for ensuring that all supporting policies and procedures necessary to comply with the Agreement are implemented within their own organisation.

9.2 Any breaches of this Agreement must be brought to the immediate attention of the other Party. The Party responsible for the breach must also advise the other Party of the breach and the outcome of any internal investigation carried out as a result. For the avoidance of doubt, a breach of this Agreement includes where the Personal Data has been lost, destroyed, disclosed, processed or used by a Party in a way that would require that Party to disclose this fact to the Information Commissioner's Office, and/or to the Data Subject, under Data Protection Law. The other Party shall provide all reasonable cooperation and assistance to the Party that has experienced a Personal Data Breach with a view to helping that Party comply with its breach reporting obligations under Data Protection Law.

9.3 Any complaint made by a Data Subject in relation to the way in which their Personal Data has been processed shall be handled, in the first instance, by the Party receiving the complaint. The Party receiving the complaint must advise the other Party of the complaint within 7 calendar days of the outcome of its investigation. If any Data Subject is not content with the outcome of the investigation, then the receiving Party should advise the Data Subject to contact the Information Commissioner's Office at the address below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate)
Email: casework@ico.org.uk

9.4 In the event that a dispute or claim is brought against a Party by a Data Subject or enforcement proceedings are taken by the Information Commissioner's Office in relation to any Personal Data processed under this Agreement, that Party shall inform and keep informed the other Party about the dispute, claim or proceedings and its progress in resolving the same. The other Party shall provide the Party being claimed against with all reasonable cooperation and assistance with a view to helping it settle the dispute or claim in a timely and amicable fashion.

10. Rectification, Blocking, Erasure and Destruction

10.1 Each Party to this Agreement is responsible for ensuring that its data protection policy covers the procedure for responding to a notice by a Data Subject, an enforcement notice by the Information Commissioner's Office, or a court order

requiring rectification, blocking, erasure or destruction of the Shared Personal Data or any other steps to be taken by that Party.

10.2 Any notice or order in terms of clause 10.1 must be dealt with by the Party that receives or is served with any such notice or order.

11. Representations and Warranties

11 Each Party represents and warrants to the other that:

11.1 it will process Shared Personal Data in compliance with Data Protection Law;

11.2 it will respond as soon as reasonably practicable to enquiries from Data Subjects and the Information Commissioner's Office in relation to Shared Personal Data and in accordance with the requirements prescribed by Data Protection Law;

11.3 where applicable, it will maintain a valid registration with the Information Commissioner's Office;

11.4 it will inform the other Party of the Data Protection Officer or individual within its organisation designated with responsibility for data protection;

11.5 the performance by it of its obligations hereunder has been duly authorised by all necessary corporate/organisational action, and this Agreement constitutes validly and legally binding obligations upon it, which are enforceable against it in accordance with their respective terms and conditions; and

11.6 the execution and delivery by it of this Agreement and the performance by it of its obligations hereunder will not:

(i) result in a breach of any provisions of its constitutional documents;

(ii) result in a breach of any agreement to which it is a party;

(ii) result in a breach of any court order or other direction given by a competent authority which is applicable to it; or

(iii) result in a breach of any applicable laws.

12. Termination

12.1 This Agreement shall be valid for a period of [x] years commencing from [DATE] (the **"Term"**).

12.2 The Term of the Agreement may be extended by the mutual written agreement of the Parties.

12.3 Unless terminated earlier under clause 12.1, or extended under clause 12.2, this Agreement shall automatically terminate on the expiry of the Term.

13. Liability and Indemnity

13.1 In fulfilling its obligations under this Agreement each Party undertakes that it (or any personnel that it engages) shall exercise reasonable skill, care and diligence and that it shall not take any actions which would result in any loss being occasioned to the other Party, a Data Subject or any third party. This Clause shall survive the termination of this Agreement.

13.2 Each Party shall indemnify and keep indemnified the other Party against all reasonable fines, penalties, liabilities, costs, expenses and damages incurred or suffered by the other Party arising from any breach by the other Party of this Agreement, unless the same are entirely due to the wilful default or gross negligence of the affected Party. Such indemnification shall not include indemnification for actions, claims, losses, demands, proceedings, fines, penalties, liabilities, costs, expenses and damages which are indirect or consequential.

14 Waiver, Amendments and Remedies

14.1 No waiver, amendment or other modification of the Agreement shall be effective unless it is in writing and signed by both Parties.

14.2 For the avoidance of doubt, the remedies provided under this Agreement are cumulative and not exclusive of any rights and remedies provided by law.

15 Assignation and Subcontracting

15.1 No Party shall assign, novate, transfer or subcontract its rights or obligations under this Agreement, or any part thereof, without the prior written permission of the other Party. Any attempt by either Party to assign, novate, transfer or subcontract any rights or obligations without such written consent of the other Party shall be void and without force and effect, and it shall not release the Party from its obligations and liabilities owed to the other Party as contained herein.

16. Illegal, Invalid and Unenforceable Terms

16.1 In the event that any one or more of the provisions contained in this Agreement are found to be invalid, illegal or unenforceable in any respect, the validity, legality or enforceability of the remaining provisions shall not in any way be affected or impaired thereby and both Parties shall mutually enter into good faith negotiations to replace the invalid, illegal or unenforceable provision, with a provision which best reflects their mutual intent and interest under the Agreement.

17. Force Majeure

17.1 Neither Party shall be liable for any damages or penalty for any delay in performance of, or failure to perform any obligation hereunder when such delay or failure is due to the elements, acts of God, earthquake, fire, flood, war

(whether declared or undeclared), terrorism, embargo, civil commotion, labour disputes, or other causes beyond that Party's reasonable control. The Party whose performance is prevented by an act of force majeure shall resume performance as soon as is reasonably practicable after the condition of force majeure is no longer operative. A Party seeking to rely on an event of force majeure ("**Force Majeure Party**") under this provision shall within five calendar days of the first occurrence of the force majeure event inform the other Party ("**the Affected Party**") of the occurrence and the manner in which performance by the Force Majeure Party has been affected.

17.2 Upon the occurrence of a condition described in clause 17.1, the Force Majeure Party shall give written notice to the Affected Party describing such affected performance, and the Parties shall promptly confer, in good faith, to agree upon equitable and reasonable action to minimise the impact on both Parties of such condition. The Parties agree that the Force Majeure Party shall use reasonable endeavours to reduce the delay caused by the force majeure events and recommence the affected performance. If the delay caused by the force majeure event lasts for more than 30 calendar days, either party may terminate this Agreement on giving 30 days' written notice of termination to the other Party under this clause.

18. Entire Agreement

18.1 This Agreement constitutes the entire Agreement between the Parties and supersedes any and all prior oral and written agreements, negotiations, representations, warranties, statements, understandings or undertakings between the Parties with respect to the subject matter hereof.

19. Independent Entities

The Parties hereby agree and undertake that they are independent entities engaged in the conduct of their own business and no Party shall be deemed to be the agent, representative or employee of the other for any purpose

whatsoever. The Parties also agree and undertake that this Agreement does not create any right or authority to make any representation or warranty or to assume, create or incur any liability or obligation of any kind, express or implied, in the name of or on behalf of the other Party.

20. DISPUTE RESOLUTION

20.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

20.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to appointed named persons, at management level, for both parties, as escalation points who will endeavour in good faith to resolve the issue.

20.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause 20.2, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

20.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 20.1 to 20.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause 21.

20.5 The provisions of Clauses 20.1 to 20.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

21. Applicable Law and Jurisdiction

21.1 This Agreement shall be governed by and construed in accordance with the laws of Scotland.

21.2 Each party agrees that the courts of Scotland shall have exclusive jurisdiction to settle any dispute in connection with this Agreement, and each party irrevocably submits to the jurisdiction of the courts of Scotland.

22. Signatories

This agreement is signed on behalf of each of the parties by its duly authorised representative as follows:-

FIRST PARTY

_____ _____

SIGNATURE NAME

_____ _____

POSITION DATE

SECOND PARTY

_____ _____

SIGNATURE NAME

_____ _____

POSITION DATE

Appendix 1 (to **Due Diligence Checks on Contractors and Suppliers**)

Information Security Questionnaire for External Contractors

Introduction

Information Security Policy requires an evaluation of third parties who process, handle or store information. This questionnaire should be completed by the person responsible for Information Security within the organisation being contracted to provide services on behalf of your organisation (denoted as 'you') or the relevant organisation or external party).

This questionnaire consists of two columns, one with the question posed to you, the second for your response. You are not to modify or delete any of the questions. If the question does not apply to the services that are to be provided, then an "N/A" in the answer response column is sufficient.

Once the questionnaire is completed, it is to be returned to XXXX.

Any questions should be directed to XXXX.

General Information

1. Company Name and address	
2. External party Website.	
3. Information Security Contact (name and phone).	
4. Your normal contact in XXXX	
5. How long have you been in the business of providing the service requested by XXXX?	
6. Number of employees.	
7. Have any independent 3rd party security reviews been performed on the organisation? If so, who performed the review and when was it performed?	
8. What information will the organisation be processing, handling or storing on behalf of XXXX? If so, what personal details such as name and address will be processed?	
9. At what address are the systems located that will be supporting XXXX's services?	
10. Do you own/manage this environment? If not, please list who does.	
11. Will you be subcontracting any work?	
12. Are you certified to any information security or quality standards e.g. ISO 27001, ISO 90001 - if so please state the scope for these standards.	

Policy & Awareness

1. Do you have a formal information security policy? If so, please provide a copy	
2. Is the policy formally approved by senior management and regularly reviewed?	

3. Who is responsible for monitoring compliance to the information security policy? Does this take place on an annual basis?	
4. How do you promote awareness of the policy for both staff and contractors (is formal training and sign off required)?	
5. Do you ensure that specific security training is provided regularly (at least annually) to your employees, contractors and temporary staff?	

Human Resources Security

1. Please describe the level of vetting you carry out on employees and third parties.	
2. Are all personnel required to sign non-disclosure or confidentiality agreements?	
3. What disciplinary process do you have to ensure that any intentional misuse of information is managed for employees or sub contractors?	
4. Describe the process in place when personnel leave in terms of retrieval of equipment or information and staff's ongoing responsibilities regarding non-disclosure.	

Sub-contractors

1. Do you have prior written consent from XXXX for any information processing by sub-contractors?	
2. Do you have a documented process for the selection and transfer of activity to sub-contractors?	
3. Do you have agreements/contracts in place to ensure that data privacy and security arrangements meet XXXX's security requirements?	
4. Do you audit your sub-contractors?	
5. Should the need arise would XXXX be allowed to conduct a security review?	

Physical Security

1. Describe the security controls protecting the location where the information is being stored (e.g. physical entry arrangements - locked server cages, guarded access, video monitoring, visitor access controls)	
2. What physical access and authorisation controls do you have for sensitive areas (areas that aren't data centres but which store or hold sensitive data e.g. comms rooms)	

3. What controls do you implement to control physical access for external party support engineers?	
4. What environmental controls do you have in place to prevent accidental loss of data, for example raised flooring, fire detection and suppression controls?	
5. Can a representative from XXXX visit your facilities to observe the physical security controls in place? (announced or unannounced)	

Operational Controls - Change & Incident Management

1. Are changes to any of your systems tested, reviewed and applied using a documented change management process? Please describe.	
2. Do you have an incident/data breach management process that is documented, approved and monitored?	
3. Do you have procedures for reporting incidents/data breaches to your clients? If so, please describe.	
4. Do you have a process for dealing with incidents that require forensic investigation?	

Risk Assessment & Asset Management

1. Do you undertake regular security risk assessments and take steps to mitigate the risks identified? Please describe process.	
2. Do you maintain an inventory of assets?	
3. Do you have a data/information classification process?	
4. Is confidential information held or transported on data storage media encrypted and protected against corruption, loss or disclosure? Please describe your arrangements.	
5. What procedures do you have for the handling and management of removable media and hard copy information in transit & storage?	
6. What back up arrangements do you have in place? How are offsite back ups secured?	
7. What procedures and mechanisms do you use for controlling and disposing of paper documents containing sensitive data?	
8. Does the secure destruction of redundant equipment and media include the secure erasure of information? Please describe process.	

Technical Controls

A. Segregation of Information Between Clients

1. What security controls are in place to keep XXXX's systems and data separate from other client data?	

B. Access Control

1. How often do you review user access to ensure that staff continue to only have the minimum access they require for their current job?	
2. What processes and systems do you have for monitoring and managing user accounts and do all systems have access controls?	
3. Do you perform regular audits on user access exceptions e.g. failed login attempts etc.?	
4. Do staff have unique identifiers on all systems?	
5. Please describe your Password Policy (length, construction, ageing, etc)?	
6. What system access auditing processes and facilities do you implement?	

C. Authentication and Authorisation

1. Do you manage servers and network devices using secure encrypted protocols?	
2. What type of authentication is required to access servers and network devices, both from on-site and remote access (e.g. passwords, SecurID)?	
3. How is access controlled to the data/information (e.g. segregation of duties) you are processing, handling or storing on behalf of XXXX?	
4. Can an employee in your company access your network remotely? If so, please describe the procedure and system requirements.	

D. Operating System Security

1. Do you have IS procedures for protecting your systems against vulnerabilities?	
2. Do you perform routine vulnerability scanning of your customer environment? If so, what tools are used?	
3. Do you have a patch management process?	
4. Is anti-virus software deployed on systems and how often are virus definitions updated?	

E. Network Security

1. Are firewalls used to protect data and systems from the Internet and other untrusted networks?	

2. Are intrusion detection/prevention systems used? Please name devices used.	
3. Are security logs monitored to detect malicious activity?	
4. Do you correlate security events from different sources?	
5. Will wireless technology be used in this environment? If so, how is this protected?	
6. Is penetration testing carried out and if so how often?	

F. Systems Development

1. Are development activities carried out in accordance with a formal methodology including definition of testing of security requirements?	
2. Are development activities performed in a test environment (isolated from the live environment) and protected against disruption and disclosure of information?	
3. Are all elements of your systems tested development phase before the system is promoted to the live environment?	
4. Do you ensure that live data is not used within test environments?	

Business Continuity Management

1. Do you have a Business Continuity Policy and Plan and how often is it tested?	
2. What were the results of your last Business Continuity test and does your organisation have any known risks in this area?	
3. Please describe your business continuity plan.	

Compliance

1. Can you confirm that all services or systems processing XXXX information are compliant with all relevant statutory, regulatory, contractual, copyright and intellectual property requirements?	
2. Can you confirm that all XXXX information containing personal information will be handled in accordance with Data Protection legislation?	
3. Has the Information Commissioner issued any assessments against you or required an undertaking to be signed? (If yes please provide further information). Have you ever had to report a breach to the data commissioner?	

4. Have internal or external auditors conducted a review of information security arrangements in the last 12 months? Can you detail any weaknesses or improvements identified?	
5. Please describe the processes in place to ensure the ongoing monitoring of your information security arrangements.	

Declaration

Signed Undertaking

This document is signed in acceptance that the signatory's organisation, and any other organisations accessing XXXX's assets on behalf of the contractor, complies with all requirements stated herein and that all the above statements are true.

Senior Officer(s) for the CONTRACTOR with responsibility for the secure handling of XXXX Infrastructure.

Signed:	
Print Name:	
Position in Organisation:	
Dated:	