EASTHALL PARK

Information Security Policy

Date of Current Review	October 2019
Date of Next Review	October 2022
Reviewed By	Management Committee

CORPORATE FIT	
Strategic Plan	✓
Risk Register	✓
Regulatory Standards	✓
Equalities Strategy	✓
Legislation	✓

On request, the Co-operative will provide translations of all our documents, policies and procedures in various languages and other formats such as computer disc, tape, large print, Braille etc. and these can be obtained by contacting the Co-operative's offices.

Easthall Park Housing Co-operative Information Security Policy

1. Introduction

1.1 Easthall Park housing Co-operative, are committed to the highest standards of information security.

1.2 Data protection legislation requires us to:

1.2.1 use technical and organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal information;

1.2.2 implement appropriate technical and organisational measures to demonstrate that we have considered and integrated data protection compliance measures into our personal information processing activities; and

1.2.3 demonstrate that we have used or implemented such measures.

1.3 The purpose of this Policy is to:

1.3.1 protect against potential breaches of confidentiality;

1.3.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse;

1.3.3 supplement our Data Protection Policy to ensure that all staff are aware of and comply with data protection legislation as part of their roles at our organisation; and

1.3.4 increase awareness and understanding within the organisation of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the personal information that they process as part of their roles.

1.4 This Policy supplements our Data Protection Policy and other relevant policies and transparency statements, and the contents of those policies and statements must be considered, as well as this Policy.

2. Definitions

For the purposes of this Policy:

business information means business-related information, other than personal information relating to housing applicants, our tenants (and their household members), factored owners, job and volunteer applicants, current and former employees and volunteers, suppliers, contractors, business contacts (including at other registered social landlords, regulators, local authorities and

	agencies), complainants, elected members, committee members, members, Residents Panel, any future scrutiny group(s) and individuals delivering services at and seeking advice and assistance from the Glenburn Centre;
confidential information	means trade secrets or other confidential information (either belonging to us or to third parties);
personal information	means information relating to an individual who can be identified (directly or indirectly) from that information; and
sensitive personal information	means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3. Roles and responsibilities

3.1 Information security is the responsibility of all our staff. Our Data Protection Officer (DPO) is responsible for:

3.1.1 monitoring and implementing this Policy;

3.1.2 monitoring potential and actual security breaches;

3.1.3 ensuring that staff are aware of their responsibilities through training and issuing guidance and communications to them; and

3.1.4 ensuring compliance with data protection legislation and guidance issued by the Information Commissioner's Office.

4. Scope

4.1 The information covered by this Policy includes all written, spoken and electronic information held, used or transmitted by or on our behalf, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

4.2 This Policy applies to all staff.

4.3 All staff must be familiar with this Policy and comply with its terms when undertaking their roles with the organisation.

4.4 Information covered by this Policy may include:

4.4.1 personal information about housing applicants, our tenants (and their household members), factored owners, job and volunteer applicants, current and former employees and volunteers, suppliers, contractors, business contacts (including at other registered social landlords, regulators, local authorities and agencies), complainants, elected members, committee members, members, Residents Panel, any future scrutiny group(s) and individuals delivering services at and seeking advice and assistance from the Glenburn Centre;

4.4.2 other business information; and

4.4.3 confidential information.

5. General principles

5.1 All our information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

5.2 Personal information must be protected against unauthorised and / or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

5.3 Staff should discuss with the DPO the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information that they access as part of their roles at the organisation.

5.4 Our information is owned by the organisation and not by any individual or department within the organisation. Our information must be used only in connection with work being carried out for the organisation and not for other commercial or personal purpose.

5.5 Personal information must be used only for the specified, explicit and legitimate purposes for which it was collected in accordance with data protection legislation.

6. Equality and Diversity

6.1 The Co-operative's Equal Opportunities policy outlines our commitment to promote a zero tolerance to unfair treatment or discrimination to any person or group of persons, particularly on the basis of any of the

protected characteristics[1]. This includes ensuring that everyone has equal access to information and services and, to this end, the Co-operative will make available a copy of this document in a range of alternative formats including large print, translated into another language or audio.

6.2 We are also aware of the potential for policies to inadvertently discriminate against an individual or group of individuals.

To help tackle this and ensure that it does not occur, best practice suggests that organisations carry out Equality Impact Assessments to help identify any part of a policy that may be discriminatory so that this can be addressed.

6.3 The Co-operative will ascertain whether each policy requires an Impact Assessment to be carried out.

7. Information management

7.1 Personal information must be processed in accordance with:

7.1.1 the data protection principles, set out in our Data protection Policy; and

7.1.2 all other relevant policies.

7.2 We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

7.3 Personal information and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with our Data Retention Policy.

8. Human Resources information

8.1 Given the internal confidentiality of personnel files, access to such information is limited to the Director and the Senior Management Team. Other staff are not authorised to access that information.

8.2 Any staff member in a management or supervisory role or involved in recruitment must keep personnel information to which they have access strictly confidential during the recruitment process, and must pass this to the Director once the recruitment process is complete.

8.3 Staff may ask to see their personnel files and any other personal information in accordance with their rights under data protection legislation.

9. Access to offices and information

9.1 Office doors and keys and access codes must always be kept secure and keys and access codes must not be given to any third party at any time.

9.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by e.g. through ground floor windows. If this cannot be avoided, then blinds should always be closed to prevent this.

9.3 Visitors must always be accompanied and never left alone in areas where they could have access to confidential information.

9.4 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains our information, then steps should be taken to ensure that no confidential information is visible.

9.5 At the end of each day, or when desks are unoccupied, all paper documents and devices containing confidential information must be securely locked away.

10. Computers and IT

10.1 Password protection and encryption must be used, on our systems to maintain confidentiality.

10.2 Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or shared with others. (note passwords changes are automatically set on our system)

10.3 Computers and other electronic devices must be locked when not in use and when staff leave their desks, to minimise the risk of accidental loss or disclosure. (note automatic lock down is set on our system after a period of inactivity)

10.4 Confidential information must not be copied onto portable media without the express authorisation of the Director and must be encrypted. Information held on any of these devices should be transferred to our system as soon as possible for it to be backed up and then deleted from the device.

10.5 Staff must ensure they do not introduce viruses or malicious code on to our systems. Software must not be installed or downloaded from the

internet without it first being virus checked. Staff should contact the Director or Business Improvement Officer for authorisation and guidance on appropriate steps to be taken to ensure compliance. (note once approval is given this requires to be downloaded via our IT support service)

11. Disposal of computers and IT equipment

11.1 IT equipment (which includes its storage media) will be disposed of by the organisation at the end of its useful life. Such equipment may store business information, confidential information and personal information and must therefore be disposed of in a secure manner to protect such information and to ensure that it cannot be accessed post disposal.

11.2 Prior to disposal, consideration should be given to whether it is possible to re-use IT equipment within the organisation, wherever possible.

11.3 If re-use is not possible, then the IT equipment must be disposed of via our IT consultant, who will remove the IT equipment from our office and arrange to have a certificate issued to us to us to confirm that it has been disposed of securely and that all storage media have been wiped and destroyed. Secure disposal means that the IT equipment is destroyed in a manner that maintains the security of the IT equipment up to the point of destruction. We will only use contractors who provide sufficient guarantees in these regards.

11.4 Staff must not attempt to wipe storage media themselves, as deleting a file does not permanently delete it and put it beyond use.

11.5 If staff have access to the organisation's IT equipment at home or use portable devices as part of their roles, then such IT equipment must be returned to the organisation for disposal and must not be retained by staff or otherwise disposed of in domestic recycling or dump facilities.

11.6 The Business Improvement Officer will maintain an IT equipment destruction register, recording details of the IT equipment that has been disposed of by the organisation (including the IT equipment's asset number) and the method of destruction), together with copies of the certificates issued by our contractor under paragraph 11.3.

12. Communications and transfer of information

12.1 Staff must be careful about maintaining confidentiality when speaking in public places e.g. when speaking on a mobile telephone.

12.2 Confidential information must be marked "confidential" and circulated only to those who need to know the information during their work for the organisation.

12.3 Confidential information must not be removed from our offices, unless required for authorised business purposes, and then only in accordance with paragraph 12.4 below.

12.4 Where confidential information is permitted to be removed from our offices, all reasonable steps must be taken to ensure that the integrity and confidentiality of the information are maintained. Staff must ensure that confidential information is:

12.4.1 stored on an encrypted device with strong password protection, which is kept locked when not in use;

12.4.2 when in paper format, not transported in clear or other unsecured bags or cases;

12.4.3 not read in public places (e.g. waiting rooms, cafes and on public transport); and

12.4.4 not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots and cafes).

12.5 Postal and e-mail addresses and telephone numbers should be checked and verified before information is sent to them. Care should be taken with e-mail addresses to ensure that Microsoft Outlook auto-complete features have not inserted incorrect addresses. (note auto complete is restricted on Computers)

12.6 All sensitive or particularly confidential information should be encrypted or password protected before being sent by e-mail or be sent by recorded delivery and its delivery tracked.

13. Personal e-mail and cloud storage accounts

13.1 Personal e-mail accounts, such as Yahoo, Google or Hotmail and cloud storage services, such as Dropbox, iCloud and OneDrive, are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.

13.2 Staff must not use a personal e-mail account or cloud storage account for our business purposes.

13.3 If staff need to transfer a large amount of personal information, they should contact the Director for assistance.

14. Home working

14.1 Staff must not take our information home unless required for authorised business purposes, and then only in accordance with paragraph 14.2 below.

14.2 Where staff are permitted to take our information home, staff must ensure that appropriate technical and practical measures are in place

within the home to maintain the continued security and confidentiality of that information. In particular:

14.2.1 personal and confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

14.2.2 all personal and confidential information must be returned to and disposed of at the office and not in domestic waste or at public recycling facilities.

14.3 Staff must not store confidential information on their home computers and devices.

15. Transfer to third parties

15.1 Third parties should be used to process our information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be "processors" for the purposes of data protection legislation. Examples of processers include our contractors, consultants and professional advisers.

15.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the DPO for more information.

16. Training

16.1 All staff will receive training on information security and confidentiality. New staff will receive training as part of the induction process. Further training will be provided on a regular basis or whenever there is a substantial change in the law or our policy and procedure.

16.2 Training is provided by the DPO and attendance is compulsory for all staff at all levels.

17. Reporting breaches

17.1 All members of staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows us to:

17.1.1 investigate the failure and take remedial steps, if necessary;

17.1.2 maintain a register of compliance failures; and

17.1.3 make any applicable notifications to the Information Commissioner's Office, the Scottish Housing Regulator and affected data subjects, if necessary.

18. Consequences of failure to comply with this Policy

18.1 We take compliance with this Policy very seriously. Failure to comply with it puts us at significant risk.

18.2 Due to the importance of this Policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under our procedures, and this action may result in dismissal for gross misconduct. If an external organisation breaches this Policy, they may have their contract terminated by us with immediate effect.

18.3 Any questions or concerns about this Policy should be directed to the DPO.

19. Review and updates to this policy

We will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.