INFORMATION SECURITY POLICY

1 Introduction

1.1 The Association is committed to the highest standards of information security.

1.2 Data protection legislation requires the Association to:

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

1.2.2 implement appropriate technical and organisational measures to demonstrate that the Association has considered and integrated data protection compliance measures into the Association's personal information handling and use activities; and

1.2.3 demonstrate that the Association has used or implemented such measures.

1.3 This purpose of this Policy is to:

1.3.1 protect against potential breaches of confidentiality;

1.3.2 ensure all the Association's information assets and IT facilities are protected against damage, loss or misuse;

1.3.3 supplement the Association's Privacy Policy to ensure that all staff are aware of and comply with data protection legislation as part of their roles at the Association; and

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

1.4 The Association will review and update this Policy in accordance with the Association's data protection obligations and the Association may amend, update or supplement it from time to time.

2 Definitions

For the purposes of this Policy:

business information	means business-related information, other than personal information relating to: housing applicants, their household members, next of kin / emergency contacts and referees; tenants and their household members; shared owners and their household members; factored owners; job applicants (and their referees), apprentices and current and former employees; contractors, consultants and service providers, including the Association's solicitors, auditors and other professional advisers; elected members, including Councillors and Members of the Scottish Parliament; business contacts at membership bodies (such as the Scottish Federation of Housing Associations), tenant support organisations, local authorities, the Scottish Government and other public bodies; Committee members; and members;
confidential information	means trade secrets or other confidential information (either belonging to the Association 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 the Association's staff. The Association's 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 the Association's 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, including employees and apprentices.

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

4.4 Information covered by this Policy may include:

4.4.1 personal information relating to: housing applicants, their household members, next of kin / emergency contacts and referees; tenants and their household members; shared owners and their household members; factored owners; job applicants (and their referees), apprentices and current and former employees; contractors, consultants and service providers, including the Association's solicitors, auditors and other professional advisers; elected members, including Councillors and Members of the Scottish Parliament; business contacts at membership bodies (such as the Scottish Federation of Housing Associations), tenant support organisations, local authorities, the Scottish Government and other public bodies; Committee members; and members;

4.4.2 other business information; and

4.4.3 confidential information.

4.5 This Policy supplements the Association's Privacy Policy and other relevant policies (including the Data Breach Management Procedure) and fair processing notices and the contents of those policies and notices must be considered, as well as this Policy.

5 General principles

5.1 All of the Association's 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 handling and use 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 Association.

5.4 The Association's information is owned by the Association and not by any individual or department within the Association. The Association's information must be used only in connection with work being carried out for the Association 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 Information management

6.1 Personal information must be handled and used in accordance with:

6.1.1 the data protection principles, set out in the Association's Privacy Policy; and

6.1.2 all other relevant policies.

6.2 The Association will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful handling and use, and against accidental loss, destruction or damage.

6.3 Personal information and confidential information will be kept for no longer than is necessary and stored and destroyed in accordance with the Association's Data Retention Policy.

7 Human Resources information

7.1 Given the internal confidentiality of personnel files, access to such information is limited to the Chief Executive. Other staff are not authorised to access that information (although line managers may have access for recruitment and disciplinary matters).

7.2 Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

7.3 Staff may ask to see their personnel files and any other personal information in accordance with their rights under data protection legislation. Further information is available in the Association's response procedures for Data Subject Requests and from the Association's DPO.

8 Access to offices and information

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

8.2 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 positioned to prevent this.

8.3 Visitors must be required to sign in at reception, always accompanied and never left alone in areas where they could have access to confidential information.

8.4 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 the Association's information, then steps should be taken to ensure that no confidential information is visible.

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

9 Computers and IT

9.1 Password protection and encryption must be used, where necessary, on the Association's systems to maintain confidentiality.

9.2 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.

9.3 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.

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

9.5 Staff must ensure they do not introduce viruses or malicious code on to the Association's systems. Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact the Association's Finance Officer, Director of Finance and Corporate Services or IT provider for authorisation and guidance on appropriate steps to be taken to ensure compliance.

10 Communications and transfer of information

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

10.2 Confidential information must be circulated only to those who need to know the information during their work for the Association.

10.3 Confidential information must not be removed from the Association's offices, unless required for authorised business purposes, and then only in accordance with paragraph 10.4 below.

10.4 Where confidential information is permitted to be removed from the Association's 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:

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

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

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

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

10.5 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 and Microsoft Outlook auto-complete features must be disabled.

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

11 Personal e-mail and cloud storage accounts

11.1 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 the Association's IT systems.

11.2 Staff must not use a personal e-mail account or cloud storage account for the Association's business purposes.

11.3 If staff need to transfer a large amount of personal information, they should contact the Association's Finance Officer, Director of Finance and Corporate Services or IT provider for assistance.

12 Home working

12.1 Staff must not take the Association's information home unless required for authorised business purposes, and then only in accordance with paragraph 12.2 below.

12.2 Where staff are permitted to take the Association's 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:

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

12.2.2 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.

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

13 Transfer to third parties

13.1 Third parties should be used to process the Association's 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.

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

14 Training

14.1 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 the Association's policy and procedure.

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

15 Reporting breaches

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

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

15.1.2 maintain a register of compliance failures; and

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

15.2 Reference should be made to the Association's Data Breach Management Procedure for the Association's reporting procedure.

16 Consequences of failure to comply with this Policy

16.1 The Association takes compliance with this Policy very seriously. Failure to comply with it puts the Association at significant risk.

16.2 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 the Association's 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 the Association with immediate effect.

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

17 Review

This policy will be regularly monitored and formally reviewed in accordance with the Association's data protection obligations and the Association may amend, update or supplement it from time to time and at least every 3 years or earlier, if required by changes in legislation.

Anne Smith

Director of Finance and Corporate Services/Depute Chief Executive

August 2019

Policy Review Consultation Process

Considered by the Management Team on	2nd September 2019
Considered by the Finance, Audit & Corporate Governance Committee on	12th September 2019
APPROVED BY THE MANAGEMENT COMMITTEE ON	**26th September 2019**
Date of Next Review	**September 2022**