TOLLCROSS
housing association

Information Security Policy

Prepared By	Anne Fitzsimons, Corporate Services Director
Policy Created	November 2018
Date of Last Review	17th December 2018
Date of Current Review	10th May 2021
Date of Next Review	December 2024
Reviewed By	Audit & Business Sub-Committee

CORPORATE FIT	
Internal Management Plan	✓
Risk Register	✓
Business Plan	✓
Regulatory Standards	✓
Equalities Strategy	✓
Legislation	✓

On request, the Association 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 Association's offices.

1. Introduction

1.1 We, Tollcross Housing Association, 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, integrity and availability;

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 procedures (including the Data Breach Management Procedure) and transparency statements, and the contents of those policies, procedures 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), sharing owners, 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, Events Focus Group, Scrutiny Group (Performance Improvement Network), and individuals delivering services at and seeking advice and assistance from the Advice and Learning Centre;
confidential information	means trade secrets or other confidential information (either belonging to us or to third parties);
personal data	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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;
Special category personal data	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 Corporate Services Director, with advice from 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), sharing owners, 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, Events Focus Group, Scrutiny Group (Performance Improvement Network), and individuals delivering services at and seeking advice and assistance from the Advice and Learning 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 Tollcross Housing Association is a data controller and as such our personal data is the responsibility of the organisation and not 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 data must be processed (used) only for the specified, explicit and legitimate purposes for which it was collected in accordance with data protection legislation and the data protection principles.

6. Equalities

6.1 An Equality Impact Assessment (EIA) has been carried out when reviewing this policy. In line with good practice the completed EIA will be published alongside the Information Security Policy.

6.2 Where there is a need for follow-up action, the tasks and timeframe for achieving them shall be noted in the Equality and Human Rights Action Plan to ensure they are addressed.

6.3 We do not see this policy as having any direct impact upon the protected characteristics contained within the Equality Act 2010.

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, procedures and our transparency statements.

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 Corporate Services Director and Finance Director. 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 Corporate Services 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. Further information is contained in our Data Subject Rights procedures and from our DPO.

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 be required to sign in at reception, always 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. Please refer to Appendix 1 of this policy for further information on the Association's 'Clear Desk Policy'.

10. Computers and IT

10.1 Password protection and encryption must be used, where available, 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.

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.

10.4 Confidential information must not be copied onto portable media without the express authorisation of the Finance Director and must be encrypted. Information held on any of these devices should be transferred to our document management system as soon as possible

for it to be backed up and then deleted from the device. Please refer to Appendix 2 of this policy for more detailed information on the Association's 'Mobile Devices Policy'.

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 Finance Director for authorisation and guidance on appropriate steps to be taken to ensure compliance.

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 contractor, who will remove the IT equipment from our office and issue a certificate to us to confirm that all personal data has been removed or 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 Finance Director 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 or using Laptops on public transport

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.

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 Finance 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 13.2 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 a Data Protection Impact Assessment (DPIA) may be required and 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 developing new processes or systems or setting up new arrangements with third parties or altering existing arrangements should consult the DPO prior to making any changes in case a DPIA is required.

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 Corporate Services Director and 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.

17.2 Reference should be made to our Data Breach Management Procedure for our reporting procedure.

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 Corporate Services Director or 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.

Appendix 1
Information Security Policy – 'Clear Desk and Clear Screen Policy'

Clear Desk

All Tollcross Housing Association staff are to leave their desk/workstation paper free at the end of the day.

All Tollcross Housing Association staff 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.

Tollcross Housing Association 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. Where possible, please use the confidential coding on the printers.

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 Tollcross Housing Association staff securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this ensures risk can be reduced.

All Tollcross Housing Association 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 should be treated with the same care.

Clear Screen

All Tollcross Housing Association staff 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', or 'ctrl, alt, delete'.

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.

Tollcross Housing Association staff 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 data.

Appendix 2
Information Security Policy - Mobile Devices

1. Introduction

This document details the requirements for the use and secure operation of portable mobile devices and removable media by Tollcross Housing Association staff. Tollcross Housing Association recognises the advantages of using portable/mobile devices provided for staff during the performance of their daily duties.

It is also recognised that Remote Access is a valuable method for staff to connect to Tollcross Housing Association's network resources, when away from our premises.

This document covers the use of all portable computing storage and remote access devices used for work purposes in order to:

- Provide secure access to the Tollcross Housing Association's information systems.
- Preserve the integrity, availability and confidentiality of the Tollcross Housing Association's information and information systems.
- Manage the risk of serious financial loss, loss of customer and public confidence or other serious business impact which may result from a failure in security.
- Comply with all relevant regulatory and legislative requirements (including Data Protection laws) and to ensure that the organisation is adequately protected under computer misuse legislation.

2. Scope

This policy applies to all officers and employees of Tollcross Housing Association, including temporary staff and agency staff, students, voluntary staff, contractors and trainees on temporary placement, as well as those persons holding honorary positions ('staff').

3. Requirements

3.1 Portable Devices

For the purpose of this policy, a Portable Device is defined as any device that may synchronise with another computer, and will include any of the following items:

- Laptop and notebook computers
- iPads / Tablets
- Smart phones including iPhones and any other mobile system that may fall into this category
- Webcams
- USB memory sticks (only for temporary storage of information, information to be transferred to secure server as soon as practicable and deleted from USB stick)
- MP3 players including iPods (must not be used at any time for storing Tollcross Housing Association's personal or commercial information)
- CDs, DVDs
- Any other item that may be utilised to store or transport data.

This list is not exhaustive. Any portable device used in connection with the organisation must be encrypted to a minimum of 256bit encryption. Further guidance may be obtained from the Finance Director in relation to what is defined as a portable media device and encryption.

3.2 Use of Own Devices

The use of staff members' own devices is not permitted.

3.3 Working Procedures

All Portable Devices issued by the organisation are to be issued to a named individual and must not be shared or used by anyone who is not recorded as the asset owner for audit purposes and to comply with Data Protection legislation.

The transfer of any Portable Device between staff members must only be done via the Finance Director. All laptops, notebooks, USB Pens, iPads and other Smartphones must be encrypted.

Documents containing personal or commercial data from the organisation's servers must not be copied without express permission of the Finance Director or another member of the Leadership Team.

Information must be protected from persons not authorised to view it. Whenever possible, Portable Devices should not be used in public areas.

3.4 Asset Management

Any business-related software applications on mobile Portable Devices must be approved, appropriately licensed and recorded on the Tollcross Housing Association licence asset register. The Finance Director will maintain a software application asset list to ensure licensing conditions are not breached. Procurement of additional software for business must adhere to the organisation's procedures, including the potential for a Data Protection Impact Assessment to be completed.

Portable Devices must not be readily identifiable as belonging to or associated with Tollcross Housing Association. If the Portable Device can be associated with the Association, this may increase the impact (e.g. risk) to the Association's reputation in the event of loss or theft. However, all of Tollcross Housing Association-owned Portable Devices must carry asset identification.

All iPads should have a Mobile device management system installed before they are issued.

Staff issued with a Tollcross Housing Association-owned encrypted Portable Device will be required to sign a declaration that they have read, understand and accepted this policy, and the conditions of use before using the device.

Upon leaving the organisation all mobile media devices must be handed back. Failure to hand the mobile media device back at the end of your employment may be viewed as theft and may result in legal action being taken against you.

3.5 Security and Passwords

Staff are personally responsible for the security of the Portable Device wherever they may be including Tollcross Housing Association's premises, the premises of other organisations, in private or public transport or at home. Staff will be liable for any cost resulting from the loss or accidental damage of the device as a result of carelessness. Where a device has been stolen, on production of a Police Crime Report, the Association will assume liability.

Staff must employ whatever security initiatives are available with the device, for example utilising the device PIN code. In addition to the individual Portable Device security features, each Portable Device must have a password enabled to access it.

4. Legislation

This document has been written to meet the requirements of:

- The Computer Misuse Act 1990
- The UK General Data Protection Regulation
- The Data Protection Act 2018

- The Privacy and Electronic Communications Regulations (PECR) 2003

Date:

Signed:

Position: