Information Security Policy

Prepared by	Dianne Mathewson, Corporate Services Manager
Policy created	November 2018
Date of last review	10 May 2021
Date of current review	13 May 2024
Date of next review	May 2027
Reviewed by	Audit & Business Sub-Committee

Corporate Fit	Internal Management Plan	✓
	Risk Register	✓
	Business Plan	✓
	Equalities Strategy	✓
	Legislation	✓

Keep in touch

868 Tollcross Road | G32 8PF
0141 763 1317
info@tollcross-ha.org.uk
www.tollcross-ha.org.uk

Registered Scottish Charity No.SC040876 | Registered with the Scottish Housing Regulator No.197 | Registered Property Factor No.PF000261 | Registered Society under Co-operative and Community Benefit Societies Act 2014 No.1798RS

Alternative formats available

Happy to translate
Możemy przetłumaczyć
Раді перекладати
Ni Fahari kutafsiri
نحن سعداء لتقديم الترجمة
अनुवाद करके खुशी हुई
ਅਨੁਵਾਦ ਕਰਨ ਵਿੱਚ ਖੁਸ਼ੀ
乐意翻译

Our policies provide a framework to underpin our vision and values, to help us achieve our strategic objectives.

Our Vision

Local people, local control.

By providing quality homes and services, we will create stronger communities and a better quality of life for our customers.

Our Values

- Focused on the needs of our customers and communities.
- Supportive of our staff and Committee members.
- Responsible, efficient, and innovative.
- Open and accountable.
- Inclusive and respectful.
- Fair and trustworthy.

Strategic Direction

Consolidation and improvement: Applicable to our core business as a landlord & property manager.

Growth: Through the new build opportunities, we are taking forward.

Partnerships: Where this can help to address shared goals and increase capacity and value.

Resilience: A key priority across all parts of our business.

Strategic Objectives

Services: Deliver quality, value for money services that meet customers' needs

Homes & neighbourhoods: Provide quality homes and neighbourhoods.

Assets: Manage our assets well, by spending wisely.

Communities: Work with local partners to provide or enable services and activities that benefit local people and our communities as a whole

Our people: Offer a great workplace environment that produces a positive staff culture and highly engaged staff.

Leadership & Financial: Maintain good governance and a strong financial business plan, to ensure we have the capacity to achieve our goals.

Our Equalities and Human Rights Commitment

We understand that people perform better when they can be themselves and we are committed to making the Association an environment where employees, customers, and stakeholders can be open and supported. We promote equality, diversity, and inclusion in all our policies and procedures to ensure that everyone is treated equally and that they are treated fairly on in relation to the protected characteristics as outlined in the Equality Act 2010.

Privacy Statement

As data controller we will collect and process personal data relating to you. We will only collect personal information when we need this. The type of information we need from you will vary depending on our relationship with you. When we ask you for information, we will make it clear why we need it. We will also make it clear when you do not have to provide us with information and any consequences of not providing this. We are committed to being transparent about how we collect and use your data, and to meeting our data protection obligations with you. Further information about this commitment can be found within our full Privacy Statements.

Policy Scope & Review

For the purpose of this policy the term Association will include all members of the Tollcross Housing Association Limited. Therefore, all employees, governing body members, volunteers, customers and other relevant stakeholders will be expected to adhere to this policy and/or procedure. All policies and procedures are reviewed every 3 years in line with best practice and current legislation. The Association reserves the right to make additions or alterations to this policy and procedure from time to time. Any timescales set out in this policy may be extended where required.

Contents

Section		Pages
1.	Introduction	2
2.	Purpose & scope	2
3.	Responsibilities	2-3
4.	Information security principles	3-4
5.	Personal devices	4-5
6.	Managing a security incident	5

Appendices		Pages
1.	Equality Impact Assessments	6
2.	Clear Desk & Clear Screen Policy Statement	7
3.	Data Breach Management Procedure	8-10
4.	Password Setting and Control Procedure	11

1. Introduction

1.1. We are committed to the highest standards of information security. Data protection legislation requires us to:

- 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.
- implement appropriate technical and organisational measures to demonstrate that we have considered and integrated data protection compliance measures into our personal information processing activities.
- demonstrate that we have used or implemented such measures.

1.2. We are aware that an increased reliance on technology means an increased vulnerability to severe security breaches, where data can be lost of compromised. This policy should be read in conjunction with our Acceptable Use Policy, which provides further information into ICT usage.

2. Purpose & scope

2.1. The purpose this policy is to protect our 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 employees understand our requirements for handling personal data and to clarify the standards of data security which we expect to be implemented.

2.2. 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

2.3. The information covered by this policy includes all hard copies 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. This policy should be read in conjunction with our Data Protection Policy.

3. Responsibilities

3.1. Below is a summary of the key responsibilities for employees, managers, and the Association. Further relevant responsibilities will be detailed within each section.

3.2. Employees are responsible for:

- Ensuring they adhere to the principles of this policy (section 4).
- Handling information safely and securely, to prevent from being unlawfully accessed, lost, wrongfully deleted or damaged.
- Reporting any security incidents as soon as they occur to the Data Protection Lead (and actively engage in any relevant investigation and learning requirements).
- Undertaking relevant training identified by the Association.

3.3. Managers are responsible for:

- Ensuring employees understand their responsibilities and actively promote the good information security practices.
- Any incidents are investigated, and learning outcomes identified and implemented.

3.4. Directors are responsible for:

- Ensuring the correct equipment and systems are in place to maximise information security.
- Developing, maintaining, and testing disaster recovery plans.

3.5. Our Data Protection Lead (with advice and assistance from our external Data Protection Officer) is responsible for:

- Recording and reviewing all security incidents.
- Managing investigations and implementing policy changes (when required).
- Notifying the ICO, data subjects, and any other relevant stakeholders (when required).

3.6. We outsource our ICT support services to an external contractor. These competent contractors are responsible for:

- Ensuring the ICT infrastructure is fit for purpose and actively monitored.
- Ensuring relevant security software is up-to-date (e.g. fireware, antivirus software).
- Recommending and implementing relevant security systems/protocols to minimise threats and potential security incidents.
- Disposing of ICT equipment no longer used by the Association (including ensuring all data is erased prior to destruction).

4. Information security principles

4.1. Below is a summary of the key information security principles that must be adhered to, this is not an exhaustive list.

4.2. Office security: Our offices are open to the public to visit. To ensure information is kept secure, you are expected to:

- Ensure visitors are always accompanied in areas where information or data is accessible (e.g. beyond reception and community areas).
- Ensure areas accessible with codes or keys, are kept secure and access not shared with an unauthorised 3rd party.
- Ensure no data is stored within shared community areas (e.g. filing cabinets).
- Store any hard-copy information within a secure / locked cabinet.
- Adhere to our clear desk and clear screen policy statement (appendix 2).
- Ensure confidential information is not left on printers (it should be collected at point of printing).

4.3. Hardware & ICT Systems: Our systems have been designed to enable you to work effectively and securely, and you are expected to use them in a safe manner by:

- Adhering to the password setting and control requirements (appendix 4).
- Never sharing passwords or asking a colleague to share their password.
- Locking screens and devices when not in use.
- Physically securing mobile devices when not in use.
- Not downloading unauthorised software or applications.

- Not connecting unauthorised devices or equipment (e.g. USBs).
- Not connecting over unsecured network or internet connections.
- Not using personal email accounts or storage for work purposes.
- Deleting malicious emails (e.g. phishing, malware), and not clicking on any links sent from unknown sources.
- Not providing login and password to any software not supplied by the Association.
- Adhering to our Acceptable Use Policy (which provides further expectations in terms of ICT systems and hardware).

4.4. Data Transfers: There may be a requirement to share or transfer information to a 3rd party or customer (e.g. subject access request). When this occurs, you are expected to:

- Ensure there is a valid reason and authorisation for the data sharing (e.g. processing agreement).
- Ensure the information is shared with the correct person or organisation (e.g. check ID, addresses, etc.).
- Ensure, where reasonably practicable, any information shared by post is kept secure (e.g. use of recorded delivery).
- Password protect or encrypt sensitive information being shared electronically.

4.5. Homeworking: There may be occasions where employees are required to work from home, in these instances, you are expected to:

- Not take home any personal or confidential information in hardcopy.
- Ensure that the internet connection is secure (password protected, etc.).
- Take precautions to ensure screens are not visible from non-authorised persons (e.g. family members).

4.6. Data disposal / destruction: Our Data Retention Policy outlines the duration we hold data and information. Once the relevant timescales have past, you are expected to:

- Destroy hardcopies of information using the secured shred bins.
- Ensure any confidential waste is not left in accessible or shared areas.
- Delete electronic information permanently (as far as reasonably possible).

5. Personal devices

5.1. We will issue ICT equipment and devices to support an employee to carry out their job role. However, we understand there may be occasions where an employee wishes to use their own device as an alternative (e.g. personal mobile phone).

5.2. We will not limit access to cloud-based systems (e.g. Microsoft 365). However, an employee must not transfer any information or data from these systems onto personal devices. They must be used for transactional purposes only (e.g. email).

5.3. Where an employee wishes to access internal systems (e.g. hosted by our servers) from their own device, they will require to have any device approved by their Director. Before approval can be given, an employee must be able to demonstrate that their device as adequate security systems in place (e.g. anti-virus software).

5.4. One approved, the device will then be required to be:

- Set up and security reviewed by our ICT support services (this may include downloading relevant software etc.).

- Reviewed and updated in line with the needs of the Association (e.g. software and security updates).
- Kept secure with password access set. If the device is lost or stolen at any point, the employee must report this to the Data Protection Lead as soon as possible.

5.5. Association information / data must never be saved onto a personal device. We consider this a serious breach of security and will be investigated in line with our disciplinary policy.

6. Managing a security incident

6.1. 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.

6.2. It is the responsibility of all employees to report any suspected or actual security incident as soon as possible to the Data Protection Lead, who will arrange for the incident to be dealt with in line with our breach procedure (appendix 3).

6.3. A Security Incident involving personal data is considered a Personal Data Breach. Some breaches of this nature must be reported to the Information Commissioner's Office, and we must notify the individuals whose personal data has been involved in the breach, under certain circumstances.

6.4. Essentially while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. Employees must not notify any individuals of a Personal Data Breach, this responsibility will sit with the Data Protection Lead or appointed investigation officer (as per the procedure in appendix 3).

6.5. A security incident can include, but not limited to:

- Unauthorised access to premises where information is stored, or to ICT systems.
- Unauthorised or inappropriate disclosure of organisation information.
- Suspected or actual breaches, compromises, or other unauthorised access to systems, data, applications, or accounts.
- Unauthorised changes to hardware / software or information / data/
- Loss or theft of ICT equipment or other data storage devices and media.
- 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.

Appendix 1 – Equality Impact Assessment

Policy	Information Security Policy		
EIA Completed by	Corporate Services	EIA Date	

1. Aims, objectives and purpose of the policy / proposal
The purpose this policy is to outline the expectations for our employees in relation to our information security and how we manage a breach.

2. Who is intended to benefit from the policy / proposal?
Employees and customers.

3. What outcomes are wanted from this policy / proposal?
To ensure all employees are aware of what is expected of them and to ensure the safety of our customers (and employees) data.

4. Which protected characteristics could be affected by proposal?			
	☐ Age	☐ Gender reassignment	☐ Religion or belief
	☐ Disability	☐ Marriage & civil partnership	☐ Sex
	☐ Race	☐ Pregnancy and maternity	☐ Sexual orientation

5. If the policy / proposal is not relevant to any of the protected characteristics listed in part 4, state why and end the process here.
The policy is a blanket approach to data security and would not be impacted by any of the protected characteristics.

6. Describe the likely impact(s) the policy / proposal could have on the groups identified in part 4

7. What actions are required to address the impacts arising from this assessment? (This might include; collecting data, putting monitoring in place, specific actions to mitigate negative impacts).

Appendix 2 – Clear Desk & Clear Screen Policy Statement

To ensure the Association adheres to data protection legislation, policy and best practice, we have adopted this Clear Desk and Clear Screen Policy Statement.

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 employees 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 employees must:

- leave their desk/workstation paper free at the end of the day.
- 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.
- ensure all sensitive and confidential paperwork is removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives.
- ensure all waste paper which contains sensitive or confidential information is placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins.
- ensure documents which are likely to be needed by other members of staff are stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals. All managers should have spare keys for all desks/workstations so that documents can be accessed if the employee is absent from work.
- 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.
- ensure sensitive information, if needed to be printed, should be cleared from printers immediately (and printers should be left clear at the end of the day).

Electronic records are accessible to unauthorised individuals where PCs, laptops, phones and other electronic devices are left unattended (and unsecured). All employees must:

- log off from their PCs/ laptops when left for long periods and overnight.
- lock their screen (PC/laptop/mobile/tablet/etc) when not in use (e.g. leaving for lunch or to attend a meeting). Employees should not rely on the automatic lock screen to ensure their screen is locked.
- set a PIN or password for any work mobile devices, or device used for work purposes.
- be aware of who can view their screens when in use and ensure unauthorised individuals do not view any information displayed.

Failure to adhere to this policy statement may result in further action in line with the Association's Disciplinary Policy.

Appendix 3 – Data Breach Management Procedure

Step 1 – Incident notification

An employee will notify the Data Protection Lead (DPL) about a suspected or actual information security incident. They must provide the following information:

- Date and time they became aware of the breach / potential breach.
- How they became aware of the of the breach / potential breach.
- Date and time the breach / potential breach occurred.
- Description of breach / potential breach.
- Any actions taken since breach / potential breach.
- Number and details of any data subject impacted.

Step 2 – Incident containment & recovery

The DPL will identify a suitable investigation officer to investigate the breach / potential breach. Before a full investigation can take place, the DPL and investigation officer must contain the breach / potential breach to ensure that no further loss, destruction, damage, or unauthorised disclosure of information / data.

The DPL and investigation officer will, as far as reasonably practicable, put in steps to stop or minimise the impact of the incident and recover, rectify, or delete any relevant information / data.

Step 3 – Assessing the risk

Before deciding on the next steps necessary, further to immediate containment, the DPL and investigation officer will assess the risks which may be associated with the incident. They will access the incident and consider if the incident:

- is a Personal Data Breach (and if the relevant individual needs to be informed).
- is reportable to the ICO, SHR, or other regulatory body.
- requires to be reported to the Police.
- requires to be reported to the insurers.

The following factors will be considered when accessing the incident:

- Type of data involved (e.g. personal, sensitive, potential for further misuse, etc.).
- Any security or protections associated with the data (e.g. encryption or password protection).
- Incident trigger (e.g. human error, criminal activity, etc.).
- Scale of incident (how many individuals could be impacted).
- Likely consequences of the incident (e.g. could it cause harm).

Step 4 – Notification to regulatory bodies

Where notifications are required, the DPL will coordinate this with the investigation officer. Consideration needs to be given to the different regulatory bodies associated with the Association, as they will each have different requirements (e.g. notifiable events for SHR).

In terms of information security, notification to the ICO must always been considered when there has been a personal data breach, 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 (e.g. result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage).

Notifications to the ICO must take place within 72-hours, and should include the following information:

- nature of the personal data breach.
- categories and approximate number of individuals concerned.
- categories and approximate number of personal data records concerned.
- description of the likely consequences of the personal data breach.
- description of the measures taken, or proposed to be taken, to deal with the personal data breach.
- where appropriate, the measures taken to mitigate any possible adverse effects.

Step 6 – Notification to data subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPL or investigation officer will notify the affected data subjects without undue delay, including:

- a description of the nature of the breach.
- a description of the likely consequences of the breach.
- 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.
- how a complaint can be raised in relation to the breach.

When determining whether and how to notify data subjects of the personal data breach we will take account of the factors set out in the table below:

Factor	**Impact on obligation to notify**
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures — in particular, measures that render the personal data unintelligible to any person who is not authorised to access it by e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject.
Whether it would involve disproportionate effort to notify the data subject.	If so, it is not necessary to notify the data subject — but we must instead issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject in any event.

Step 7 – investigation and evaluation

Once the breach has been dealt with in terms of notification and immediate response, the investigation officer (supported by the DPL) should conduct a thorough investigation into the circumstances which led to the breach. Areas they should investigate should include:

- Reviewing security measures in place when the breach occurred.
- Identifying any failings in systems, policy or process which contributed to the breach.
- Assess whether any measures can be implemented to prevent the breach happening again.
- Identify key areas of learning required for the Association and employees.

Step 8 – reporting and review

Once the investigation is complete, the learning from investigation report should be embedded to help reduce the likelihood of a similar incident occurring again. The DPL will lead any relevant changes to policy and process required.

All information gathered throughout the investigation process will be added to the register of security breaches by the DPL. This will allow for trends and fundamental failings to be identified and in turn dealt with.

Appendix 4 – Password Setting and Control Procedure

The purpose of this procedure is to ensure that passwords, the first line of protection for employee accounts, remain safe and secure.

Passwords should be unique for software and hardware.

Employees should not repeat or reuse passwords.

Employees should avoid using personal details when setting passwords.

Passwords must not be written down or shared (even with colleagues).

Passwords must be periodically renewed (when prompted).

Passwords must adhere to an acceptable level of complexity (e.g. special characters).

All passwords must be changed immediately if:

- they are suspected of being disclosed or known to have been disclosed to anyone.
- there is a suspected breach of security linked to an employee's ICT account.