Data Protection Policy

Prepared by	Dianne Mathewson, Corporate Services Manager
Policy created	//
Date of last review	9 November 2020
Date of current review	4 December 2023
Date of next review	November 2025
Reviewed by	Audit & Business Sub-Committee

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

HAPPY TO TRANSLATE

Get in touch
0141 763 1317 | www.tollcross-ha.org.uk | info@tollcross-ha.org.uk
Tollcross Housing Association | 868 Tollcross Road | Glasgow | G32 8PF

If you require this document in an alternative format, please contact info@tollcross-ha.org.uk.

Braille | BSL | Audio | Large Print | Visually impaired

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

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

1. Introduction

1.1. Tollcross Housing Association (referred to herein as the Association) is a Data Controller registered with the Information Commissioner's Office (Registration No: Z6608328).

1.2. We are committed to ensuring the lawful, fair and transparent management of personal data. This policy sets out how we will do this in line with data protection legislation, best practice, and our obligations as a Registered Scottish Landlord.

2. Purpose and scope

2.1. The purpose of the policy is to ensure that employees understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access during their work with us.

2.2. This policy applies to all personal data held by the Association that relates to living identifiable individuals regardless of the category of data or the format of the data. It applies to personal data held or accessed on the Association 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.

3. Responsibilities

3.1. All employees, members, volunteers and other stakeholders (referred to as 'personnel' for the remainder of the policy), have a responsibility to ensure compliance with this policy which set out our 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).

3.2. The Management Committee are ultimately responsible for ensuring that the Association meets its legal obligations. Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

3.3. All personnel, accessing or otherwise processing personal data controlled by the Association 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.

3.4. Our Data Protection Lead, with advice and assistance from the Data Protection Officer, 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.

3.5. Employees must:

- only access the personal data that they have authority to access, and only for authorised purposes.

- only allow other employees to access personal data if they have appropriate authorisation.
- only allow third parties to access personal data if they have specific authority to do so;
- ensure that any sharing of personal data complies with the privacy statement provided to data subjects and the third party with whom it is shared agrees to put appropriate security measures in place to protect the personal data.
- keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other appropriate precautions).
- not remove personal data, or devices containing personal data (or which can be used to access it), from our premises, unless appropriate security measures are in place (such as encryption or password protection) to secure the data and the device.
- not store personal data on local drives or on personal devices that are used for work purposes.
- report any (actual or suspected) data protection failure or breaches to the Data Protection Lead.
- adhere to the Association's clear desk and screen statement (appendix 2).

3.6. We will ensure that employees are adequately trained regarding their data protection responsibilities. Employees whose roles require regular access to personal information will receive additional training to help them understand their duties and how to comply with them. All 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.

4. Definitions

4.1. 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.

4.2. We process personal data about a number of categories of data subjects, including 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, for a number of specific lawful purposes relevant to our activities and functions as a public authority and registered social landlord in Scotland.

4.3. Summary of key terms:

4.3.1 Data subject: means an individual to whom the personal data relates.

4.3.2 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 name, etc..

4.3.3 Processing: means obtaining, recording, organising, storing, amending, retrieving, disclosing and / or destroying personal information, or using or doing anything with it.

4.3.4 Special category data: means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning the health or data concerning a natural person's sex life or sexual orientation.

4.3.5 Data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.3.6 Privacy statement: statement informing data subjects about what personal data we process about them, how we gather the personal data (e.g. if through a third party), and what we use their personal data for (e.g. housing applications).

5. Compliance and principles

5.1. We will comply with our legal obligations and the data protection principles by ensuing that personal data is:

5.1.1 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.

5.1.2 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 the Association wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing.

5.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Association 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 the Association 's Retention Policy. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

5.1.4 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.

The Association 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.

5.1.5 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.

The Association 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.

5.1.6 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.

The Association 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. The Association personnel will keep data secure by taking sensible precautions and following the relevant Association policies and procedures relating to data protection.

5.2. In addition, we 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.

5.3. Further information about our basis for process personal and special category data can be found in appendix 3.

6. Individual Rights

6.1. We will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Subject Rights Procedures. We 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. We 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') – We 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 – We 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.

7. Data Sharing

7.1. In certain circumstances we 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.

7.2. 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. Further information about our data sharing agreements can be found in appendix 4.

7.3. Prior to sharing personal data, we will consider any legal implications of doing so. Data Subjects will be advised of data sharing via the relevant the Privacy Notice.

8. Data Processors

8.1. Where we engage Data Processors to process personal data on our behalf, we will ensure that:

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

9. Data Protection by Design

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

9.2. 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).

9.3. 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 the Association 's DPIA Procedure.

10. Security Incident & Breach Management

10.1. We will use appropriate technical and organisational measures (based on our size, available resources, volume of personal data processed and risks) to keep personal data secure, and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. However, occasionally we 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.

10.2. 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.

10.3. All security incidents and personal data breaches will be managed in accordance with the Association 's Information Security Incident and Personal Breach Management Procedure. To assist with the prevention of personal data breaches, all Association personnel must adhere to the Association 's Information Security Policy and procedures.

10.4. Any breaches in policy may be dealt with in line with the Association's Disciplinary Policy.

11. Monitor and review

11.1. We will regularly monitor and audit our policy and process to ensure compliance with legislation and best practice.

11.2. 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.

Appendix 1 – Equality Impact Assessment

Policy	Data Protection Policy		
EIA Completed by	Corporate Services	EIA Date	Dec 2023

1. Aims, objectives and purpose of the policy / proposal

The purpose of the policy is to ensure that employees understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access during their work with us, and any data subjects understand what can be expected from the Association (as a data controller).

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

Customer, employees and any other data subjects.

3. What outcomes are wanted from this policy / proposal?

To ensure all employees, customer and any other stakeholders understand what is (1) expected of them and (2) what they can expect from the Association.

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.

While we may collect some special category data. The actual process and policy does not have a direct impact on any 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 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.
- ensure 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.
- ensure 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 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 – Basis for processing personal data

In relation to any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

1. review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing i.e.
   - that the data subject has consented to the processing;
   - that the processing is necessary for the performance of a contract between us and the data subject;
   - that the processing is necessary for compliance with a legal obligation to which we are subject;
   - that the processing is necessary for the protection of the vital interests of the data subject or another person; or
   - that the 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;
   - that the processing is necessary for the purposes of our legitimate interests or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject;
2. except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
3. document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
4. include information about both the purposes of the processing and the lawful basis for it in our relevant transparency statement(s);
5. where special category personal data is processed, also identify a lawful basis for processing that information (see below), and document it; and
6. where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether our legitimate interests are the most appropriate basis for lawful processing, we will:

1. conduct a legitimate interests' assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
2. if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
3. keep the LIA under review, and repeat it if circumstances change; and
4. include information about our legitimate interests in our transparency statement(s).

Special category personal data is sometimes referred to as “sensitive” personal data. We may from time to time need to process special category personal data as part of our activities and functions as a registered social landlord in Scotland. We will only process this if:

1. we have a lawful basis for doing so as set out above; and

2. one of the legal bases for processing special category personal data applies e.g.

   - the data subject has given explicit consent;

   - the processing is necessary for the purposes of exercising the employment law rights of the data subject or our employment law obligations;

   - the processing is necessary to protect the data subject’s vital interests, and the data subject is physically incapable of giving consent;

   - processing relates to personal information which is manifestly made public by the data subject;

   - the processing is necessary for the establishment, exercise or defence of legal claims; or

   - the processing is necessary for reasons of substantial public interest.

Before processing any new special category personal data, staff must notify Data Protection Lead of the proposed processing, in order that the DPO may be consulted to assess whether one of the above legal bases applies. Special category personal data will not be processed until:

1. the assessment referred to in paragraph 6.5 above has taken place; and

2. the data subject has been properly informed (by way of transparency statement) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

We do not carry out automated or electronic decision-making (including profiling) based on a data subject’s personal data.

Our transparency statements set out the types of personal data that we process, what it is used for and the lawful basis for the processing.

Consent is one of the lawful bases for processing personal data and for processing special category personal data, Explicit Consent.

A data subject consents to processing of their personal data if they indicate agreement either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be enough. If consent is given in a document which deals with other matters, then consent must be kept separate from those other matters. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

Appendix 4 – Data Sharing Agreement Information

Where we use external organisations to process our personal data on our behalf, such as our contractors and service providers, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security our of personal data. Compliant data sharing agreements, data processor agreements and/or contracts must be put in place with external organisations and these must provide that:

1. the organisation may act only on our written instructions;

2. employees of the organisation processing the personal data are subject to a duty of confidence;

3. appropriate measures are taken to ensure the security of processing;

4. sub-contractors are only engaged by the organisation with our prior consent and under a written contract;

5. the organisation will assist us in providing subject access and allowing data subjects to exercise their data protection rights;

6. the organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and DPIAs;

7. the organisation will delete or return all personal data to us as requested at the end of the contract; and

8. the organisation will submit to audits and inspections, provide us with whatever information we need to ensure that they are meeting their data protection obligations, and tell us immediately if the organisation is asked to do something that could breach data protection law.