ICT Acceptable Use Policy

Prepared by	Dianne Mathewson, Corporate Services Manager
Policy created	March 2025
Date of last review	June 2013
Date of current review	March 2025
Date of next review	March 2028
Reviewed by	Management 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

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

1. Introduction

1.1. We provide a range of Information and Communication Technology (ICT) packages and equipment to allow our employees to carry out their job role effectively and efficiently.

1.2. We are aware that an increased reliance on technology means an increased vulnerability to security breaches and misuse. This policy outlines the level of acceptable use for our ICT and should be read in conjunction with our Information Security Policy, Data Protection Policy, and Data Retention Policy.

2. Purpose & scope

2.1. This policy sets out the rules expected of employees, volunteers and other 'users' when using the Association's ICT, to ensure we provide professional, accessible, and efficient services to our customers, while remaining legally compliant (a summary of the relevant legislation can be found in Appendix 2).

2.2. This policy relates to the use all of the Association's information and communication technologies (ICT), including but not limited to, telephone, email, mobile, computers, laptops, tablets, internet, and social media (further information can be found in our Social Media Policy).

2.3. This policy should be read in line with the Association's Customer Service Standards Policy. This outlines the requirements of usage specific to customers (e.g. call pick up, out of office, etc.).

3. Responsibilities

3.1. Our ICT systems may not be used directly or indirectly by employees, volunteers, or governing body members:

3.1.1 For the download, creation, manipulation, transmission, or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.
- unsolicited "nuisance" emails.
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of another member of staff or a third party.
- material which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation.
- material with the intent to defraud or which is likely to deceive a third party.
- material which advocates or promotes any unlawful act (including breaching copyright legislation).
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or material that brings the Association into disrepute.
- harmful, or non-approved, software or programmes (e.g. viruses, spyware, etc.).
- personal data, screensavers or wallpapers.

3.1.2 For the purpose of:

- intentionally wasting our resources or disrupting the work of the Association.
- corrupting, altering or destroying another data without consent or authorisation.
- denying reasonable access to our network and services.
- pursuance of commercial activities, conduct business or make personal gains (e.g. gambling websites).
- gaining unauthorised access to parts of the network or giving unauthorised access to others.
- intentionally breaching security controls (e.g. introducing spyware, viruses, or other malicious software).

3.2. Employees are responsible for the physical safety of equipment they use and must treat this with due care. Where damage is either purposeful or a result of gross carelessness, an employee may be liable to pay for the replacement or repairs of the equipment.

3.3. Employees are expected to carry out relevant training and operate all ICT equipment with due care and attention (to both the physical and virtual safety required).

4. Acceptable Use Principles

4.1. Below is a summary of the acceptable use principles for our ICT equipment and software, this is not an exhaustive list.

4.2. Email: We consider any emails sent from an employees' work account as formal and professional correspondence. Employees must:

- Take care with content and format, to ensure that it is the same level of professionalism as would be expected from formal correspondence (e.g. letters) and to avoid misunderstandings.
- Ensure adequate security measures are in place when sending sensitive information (e.g. password protection).
- Ensure that all external emails are sent with a correct and up-to-date email footer (e.g. contact details, disclaimer, etc.).
- Adhere to the Association's Customer Service Standards Policy when using email systems (e.g. replying to emails in an agreed timescale, don't' use capitals etc.).
- Use the out of office tool to indicate periods of time where email access is unavailable (e.g. annual leave, training, etc.). Out of office messages should include the duration of time and alternative contact details.
- Avoid sending large documents via email. Where possible alternative methods of sharing should be used (e.g. shared drive).
- Ensure when multiple users are being send an email, email addresses are kept confidential (e.g. blind copy).
- Review and delete emails to ensure data storage is kept to a manageable limit.

4.3. Internet: it may be necessary to use the internal on a regular basis to access certain Association ICT systems (e.g. cloud-based technology). Where usage is out-with this requirement, employees must:

- Limit usage to an acceptable level for the duration of the task.
- Only use for work-purposes during working hours (employees may access for personal use during unpaid breaks).

4.4. Telephony: we provide both desk and mobile phones to allow for employees to carry out their duties. Employees must:

- Limit personal usage and where personal use exceeds the paid contract, employees will be held responsible for payment.
- Adhere to the Association's Customer Service Standards Policy and respond to calls quickly and professionally. We actively promote group pick up, where an employee may be expected to pick up calls for the colleagues.

4.5. Shared drive: we provide ICT systems with in-built storage systems (e.g. housing management system) to allow employees to carry out their duties and reduce the amount of data to be stored independently. Where data is required to be stored out with these systems, employee must:

- Store all relevant data on the Association's centralised shared drive. Data should not be stored locally on PCs, laptops, any mobile device, or on mobile data storage devices (e.g. USBs).
- Critically assess the need for storage of the data and only store relevant data.
- Save data to the correct folder / location relating to the content of the data (to ensure the correct security levels are assigned).

5. Mobile phones

5.1. We will provide mobile phones and contracts for specific job roles. These phones remain the property of the Association and employees should use due care and attention when using them.

5.2. The contract will provide adequate data and call allowance to carry out job roles within our geographical area. Where excessive usage is identified, the employee will be liable to pay any non-work-related calls or data usage (including roaming charges associated with using the phone abroad).

5.3. Employees must adhere to legislation in relation to mobile phone usage (e.g. using hand-held devices when driving). The Association's does not expect employees to answer calls while driving and would recommend calls to be delt with at an end of journey.

5.4. All mobile telephones should be kept securely, and appropriate security measures should be taken to ensure that they, or data held on them, are not subject to loss, damage or unauthorised access.

6. Monitoring & misuse

6.1. All ICT systems are monitored for their safety and security, this includes any data stored or shared using our systems. This includes call recordings from our telephone system (these calls are held securely for 30-calendar days before being destroyed).

6.2. While we do not actively use our ICT systems for surveillance of our employees conduct and behaviour, we will use them to investigate any complaints or concerns over misuse or poor performance.

6.3. Where misuse or misconduct by an employee is identified through an investigation (as stated in point 6.2, we will further investigate the employee's conduct and behaviour in line with the Association's Disciplinary Policy (and may result in subsequent disciplinary action). This may result evidence being sought from the relevant ICT systems.

6.4. For the purpose of call recordings, we will only access this data to (1) establish the facts surrounding a complaint, (2) investigate an allegation of nuisance or abusive calls, and (3) identify any training needs.

6.5. Requests for data or recordings must be put in writing (email) from the relevant line manager to (1) Finance Director for data held on IT systems and servers or (2) Corporate Services Manager for call recording data.

Appendix 1 – Equality Impact Assessment

Policy	ICT Acceptable Use Policy		
EIA Completed by	Corporate Services	EIA Date	

1. Aims, objectives and purpose of the policy / proposal
This policy sets out the rules expected of employees, volunteers and other 'users' when using the Association's ICT, to ensure we provide professional, accessible, and efficient services to our customers, while remaining legally compliant.

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

3. What outcomes are wanted from this policy / proposal?
To ensure all ICT users are aware of what is expected of them in terms of accessing and using our ICT equipment and systems.

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 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 – ICT Related Legislation

In addition to Data Protection and Equality legislation, the following were considered as part of this policy. As legislation and case law in this area is subject to frequent change this document provides a summary and is not an exhaustive list.

The Criminal Justice and Licensing (Scotland) Act 2010 makes it an offence to display in a public place, publish, sell or distribute obscene material or (with a view to its eventual sale or distribution) make, print or keep any obscene material which includes a computer disc and any form of recording of a digital image. Where material consists of data stored electronically publishing includes transmitting that data.

The Communications Act 2003 makes it an offence to dishonestly obtain electronic communication services (illegal downloading, file sharing etc.), possess or supply any equipment that may be used for illegally obtaining electronic communications and the improper use of public electronic communications (sending grossly offensive or indecent material, sending a false message for the purpose of annoyance/anxiety to another etc.)

The Computer Misuse Act (1990) was introduced to secure computer material against unauthorised access or modification. Three categories of criminal offences were established to cover the following conduct:

1. Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer.
2. Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking.
3. Unauthorised modification of computer material, which includes, intentional and unauthorised destruction of software or data, the circulation of 'infected' materials on-line and an unauthorised addition of a password to a data file.

The Telecommunications Act (1984) and the Interception of Communications Act (1985) make it illegal to communicate any information of an indecent, obscene or menacing character by a public telecommunications system, or to misuse or tap a telecommunications system.

The Copyright, Design and Patents Act (1988) is applicable to all types of creations, including text, graphics and sounds by an author or an artist. Any unloading, downloading or printing of information through online technologies, which is not authorised by the copyright owner will be deemed to be an infringement of their rights.

Defamation Act (1996) consists of the publication of an untrue statement (which can include an opinion), which adversely affects the reputation of a person or a group of persons. If such a statement is published in a permanent form, as is the case with statements published on the Internet, including messages transmitted by email, an action for libel may be brought against those responsible.

Obscene Publications Act (1959) relates to any material which it may consider pornographic, excessively violent or which comes with the provisions of the Protection of Children Act (1978) or the Criminal Justice Public Order Act (1994).

Terrorism Act 2006
The Terrorism Act 2006 makes it an offence to encourage terrorism and to distribute terrorism material through any media. The Act allows the police the right to serve a take-down notice on any providers of electronic communications to remove any material that directly or indirectly promotes terrorism.