CCTV Policy

Prepared by	Dianne Mathewson, Corporate Services Manager
Policy created	4 August 2020
Date of last review	10 May 2021
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	✓

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

HAPPY TO TRANSLATE

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

Braille | BSL | Audio | Large Print | Visually impaired

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 are committed to the safety of our employees, customers, and visitors. We own and operate CCTV and other forms of surveillance systems at various premises, including offices and car parks. We do this for the purpose of enhancing security where we consider there to be a potential threat to the health, safety and wellbeing of individuals and to assist in the prevention and detection of risk of crime or anti-social behaviour.

1.2. We acknowledge the obligations incurred in operating such systems and the rights and freedoms of those whose images may be captured. We are committed to operating them fairly and within the law at all times and in particular will comply with the requirements of the UK General Data Protection Regulations (the 'UK GDPR') and UK Data Protection Act 2018 (the 'DPA 2018').

1.3. Our policy and procedure incorporates standards and practices from the Information Commissioner's Office Code of Practice, 'In the picture: A data protection code of practice for surveillance cameras and personal information' as well as the Surveillance Camera Commissioner Code of Practice 'A guide to the 12 principles'.

2. Purpose & scope

2.1. The purpose of this policy is to provide transparency for our employees, customers, and visitors in relation to how we use CCTV, how it is monitored, and their rights under the relevant legislation.

2.2. CCTV systems are installed and operated by us for the following purposes:

- to protect and enhance the security of our premises and assets;
- to safeguard against intrusion, vandalism, damage, disruption and anti-social behaviour;
- when requested, to assist the Police in the prevention and detection of crime;
- to provide a safer environment for employees and visitors;

2.3. This policy governs our approach to installing and operating CCTV and other forms of surveillance systems and handling the information obtained. It is underpinned by the following key principles:

- We know what the system is used for and review of its use;
- That we have completed a Privacy Impact Assessment (PIA) and this is published on our website via the Publication Scheme. Systems will only be installed with due consideration to the privacy impacts of doing so;
- That we will ensure clear signage is in place, with a published point of contact to deal with queries and complaints;
- There is clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used, and staff are aware of their responsibilities for CCTV;
- Clear rules, policies and procedures are in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them;
- That we have a policy for keeping the CCTV images we hold, and we ensure they are deleted once they are no longer needed;
- That we have a clear process for who can access the images, and a policy on disclosure;
- That the system we use follows recognised operational and technical standards. Systems will be appropriately specified and professionally installed, having due regard to appropriate technical and legal advice and other relevant guidance;

- Systems will only be installed where there is a clear identified and documented need;
- Systems will only be installed with due consideration to all alternative options;
- Appropriate technical and organisational measures will be employed to ensure the security of our systems and personal data, including relevant controls to govern access to and use of images;
- Appropriate measures will be taken to provide clear and accessible privacy information to individuals whose personal data is processed by systems;
- That we are clear on when CCTV images will be produced for criminal justice purposes;
- This policy will be supplemented by procedures, which provide detailed operational guidance on the installation, operation, use and maintenance of our systems.

3. Responsibilities

3.1. For the purposes of the UK GDPR, Tollcross Housing Association is the data controller and is legally responsible for the management and maintenance of the CCTV systems installed and operated on our premises. We will operate CCTV systems and handle any recorded images in accordance with our Data Protection Policy and these procedures.

3.2. Our Maintenance Manager is responsible for overall management and operation of the CCTV systems, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this procedure including Data Protection Impact Assessments (DPIAs). An inventory of CCTV systems in operation, including details of camera numbers and positions will be maintained. The CCTV systems are operational 24 hours a day and are capable of being monitored live at any time.

3.3. Our Data Protection Officer will advise on and review relevant documentation in relation to CCTV (e.g. Data Protection Impact Assessment, Policy, etc.).

3.4. All employees who need to use CCTV systems will be trained in respect of the necessary operational and administrative functions associated with the CCTV system operation.

3.5. We consider any attempted or actual misuse of CCTV or other surveillance systems or images by employees to be a disciplinary matter, which will be handled in accordance with the Association's disciplinary policy.

4. Installation and Surveillance

4.1. We recognise that using CCTV and other surveillance systems can be privacy intrusive. As such we will not install systems as a routine response to incidents of a criminal or anti-social nature. Notwithstanding this, we acknowledge the potential value of these systems as both a deterrent and a means of detection and will consider all potential installations on a case-by-case basis. In doing so the aim will be to demonstrate that installation is a justified, proportionate, and effective solution to an identified problem or risk.

4.2. The impact on people's right to privacy and the availability of alternative and less intrusive options will be a key consideration. To this end, all potential installations will be subject to a Data Protection Impact Assessment (DPIA). All DPIAs will be conducted, recorded and signed off in accordance with our DPIA procedures. These have been developed in accordance with Information Commissioner's Office (ICO) guidance and prescribe the approach to be followed in identifying and assessing data protection risks, and in consulting with those whose privacy is likely to be affected, where appropriate.

4.3. We will maintain a register of Data Protection Impact Assessments as a record of decision making, installation authorisation and review for CCTV. In the interests of transparency, the register and individual DPIAs shall be made publicly available on request.

5. System Specification & Installation

5.1. We will procure and site systems in accordance with an agreed standard specification, which reflects recommended practices and incorporates privacy by design features.

Relevant criteria will include, but not be limited to:

- Ensuring personal data can be easily located and extracted;
- Ensuring images are of an appropriate quality, relevant to their purpose;
- Ensuring that the date and time images are captured is easily identifiable;
- Ensuring that unnecessary images are not viewed or recorded;
- Ensuring that relevant retention periods can be complied with;
- Installing image only systems, which have no sound recording capability, as standard;
- Siting cameras to ensure only areas of interest are subject to surveillance and to minimise viewing areas not relevant to the purposes the system was installed for, with due regard given to planning permission requirements as necessary;
- Siting cameras to ensure they can produce quality images taking into account the environment where located;
- Siting cameras and equipment in secure locations, protected from unauthorised access and possible vandalism; and
- No cameras forming part of the system will be installed in a covert manner; and cameras which may be covered to protect them from weather or damage, would not be regarded as covert provided that appropriate signs are in place.

5.2. We will engage the services of specialist contractors, in accordance with relevant procurement procedures, to advise on technical specifications and system configuration and design; and to carry out installation and maintenance. Such contractors will be required to demonstrate the appropriate credentials, expertise, and understanding of the Association and data protection requirements.

5.3. We will maintain a record of all system installations, detailing location and installation date, relevant technical specifications and system design features.

6. Access and Use of Images

6.1. Access to all equipment and images will be strictly controlled. Appropriate security measures will be in place to ensure entry to physical locations is limited to authorised personnel. As a general rule, such authorised personnel will be individuals appointed by the Association and specialist contractors, acting under explicit instruction. We will have in place a written data processing agreement with these contractors which is UK GDPR compliant and clearly defines obligations, responsibilities and liabilities.

6.2. The specialist contractors will be responsible for setting and maintaining relevant technical security controls for each system, including passwords or access codes and for maintaining physical and digital access logs.

6.3. We consider the following to be permitted reasons for monitoring:

- Prevention and detection of unacceptable behaviour, including aggressive or abusive actions, towards employees on our premises;

- Prevention and detection of unauthorised access to, or other criminal activity within, our premises; and/or
- General compliance with relevant legal obligations, regulatory requirements and our policies and procedures.

6.4. We shall not undertake routine monitoring of images captured in Association locations.

6.5. Access to images will be on an as required basis and in accordance with the purpose for which the system was installed. This will only be carried out where an incident has been reported that requires investigation or where there is clear suspicion that an incident has taken place. Where it is required to access or download recorded images in order to investigate an alleged incident a data request, authorised as a minimum by the relevant manager, will be recorded in the CCTV Access Register.

6.6. Access to images may also be required in order to respond to a Subject Access Request (SAR). All requests for system footage by individuals will be treated as SARs and handled in line with our SAR procedures. In doing so we acknowledge the requirement to balance the rights of data subjects against those of other individuals who appear in the requested images. On receipt of a SAR, arrangements will be made to retain, and prevent automatic deletion of, all images of the individual submitting the SAR that have been captured.

6.7. The general principle will be that requests for images will be authorised as a minimum by the relevant manager. Images will be supplied direct to the manager that authorised the request, and receipt will be logged in the CCTV Access Register.

6.8. Disclosure of information from systems will be controlled and consistent with the purpose(s) for which the system was installed. As such disclosure is likely to be limited to law enforcement agencies or the Association's legal advisers. The CCTV Access Register will contain relevant details of image disclosure, including named recipient and reason for disclosure. Any disclosure of images must be done by secure means.

6.9. We will not routinely keep copies of images obtained through CCTV or other surveillance systems. Any images that are returned following disclosure will be disposed of securely in accordance with our Data Retention and Destruction Policy and Procedures (this will not usually exceed 30 days unless requested by the Police or other statutory enforcement agencies when, in accordance with data protection laws, the Association may retain digital images for longer periods until such time as they are able to be viewed or shared with the relevant body).

6.10. We will consider requests from Police and other legal authorities when suitable reasons have been given and that are in line with their obligations under the Investigatory Powers Act 2016. Such disclosure of information must follow our disclosure procedure.

6.11. We will not use CCTV to actively monitor employee activities. However, we will access relevant CCTV where we receive an allegation of misconduct regarding an employee (and the location of misconduct is covered by our CCTV systems). The images captured may be used as part of a disciplinary investigation process (in line with our disciplinary policy).

6.12. Where CCTV is accessed for a legitimate reason and through reviewing the images captured potential misconduct by an employee has been identified, a disciplinary investigation will be triggered to investigation the misconduct allegations.

7. Reviewing installations

7.1. As a minimum, each system will be reviewed 6 months after initial installation and every 12 months thereafter to ensure its continued use serves a legitimate purpose and is required; and that the installation specification and design is appropriate to this purpose. This will involve a review and, as necessary, an update of the DPIA to reflect changes or actions required. We have implemented review procedures.

7.2. Where it is determined that a system is no longer needed, arrangements for decommissioning will be made promptly. This will involve removal of all cameras and associated equipment and signage in accordance with our CCTV and surveillance system procedures.

7.3. Notwithstanding these regular reviews, we will separately instruct our contractors to undertake periodic maintenance and security checks. Any works to repair or replace system components, or to amend system configuration or design will be carried out only under explicit instruction.

8. Privacy information

8.1. We shall be as transparent as possible in our usage of CCTV and surveillance systems, and our Privacy Notices will reference the collection of personal data via systems. Clear and prominent signage will also be in place where systems are in operation. Signage requirements will be included as part of the standard system specification, and the appointed specialist contractors will be required to confirm these have been met as part of the installation process. In accordance with good practice these will state the general purpose for which the system is being used and contain relevant contact details where any enquiries should be directed. In this regard, complaints about implementation of or compliance with this policy or the associated procedures, will be handled in accordance with our Complaints Handling Procedure.

8.2. We acknowledge that individuals also have the right to complain to the Information Commissioner's Office (ICO) directly if they feel we are not operating CCTV and surveillance systems in accordance with the UK GDPR and/or DPA 2018.

9. Freedom of Information

9.1. As a public authority, we are subject to the Freedom of Information (Scotland) Act 2002 (FOISA). FOI requests in relation to CCTV can include information on where cameras are sited, functionality, and whether they were operational over particular time periods.

9.2. All FOI requests have to be submitted in a recordable format, e.g., by letter or email. Requests for information must be processed within 20 working days from the date of the request.

9.3. Access to CCTV images may be subject to an exemption under Section 38 (Personal Information) or section 39 (Health, Safety and the Environment) of FOISA 2002.

10. Monitor and review

10.1. Regular monitoring will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy and associated procedures. 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	CCTV Policy		
EIA Completed by	Corporate Services	EIA Date	

1. Aims, objectives and purpose of the policy / proposal
The aim of this policy is to provide a clear framework for the Association's use of CCTV.

2. Who is intended to benefit from the policy / proposal?
Customer, employees and visitors.

3. What outcomes are wanted from this policy / proposal?
To create a culture of transparency in relation to the Association's use of CCTV.

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.
CCTV is not actively monitored and is only used for specific purposes (not relating to 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).

Signed: _____ (Job title): _____
(Responsible for Policy Review)

Signed: _____ (Job title): _____
(Peer Review Confirmation)

Please attach the completed document as an appendix to your proposal report