transform housing & support

Registered office: Bradmere House, Brook Way, Leatherhead, Surrey KT22 7NA
www.transformhousing.org.uk ■ info@transformhousing.org.uk
Registered charity: 264133 ■ **Company limited by guarantee registered in England and Wales:** 01057984
Registered with the Regulator of Social Housing: H2452

Policy and procedure

Close-Circuit Television (CCTV)

Policy author (name and title)	Mandy Arnold – Head of Governance & Assurance
Executive approval date	5 February 2025
Audit & Risk Committee approval date	11 February 2025
Review frequency	3 years (unless legislation changes impose earlier revision)
Next Review Date	February 2028
Version number	2.0 Updated policy following installation of cloud-based CCTV system
Has this policy been discussed at the Client Forum? (if applicable)	Not Applicable
Who does this policy apply to?	All staff

The following documentation can be relied on to support this policy:

Data Protection Act 2018 (DPA)

UKGDPR (UK General Data Protection Regulation)

EDPB (European Data Protection Board)

Values

Respect	Empowerment
▪ Value diversity and fairness ▪ Act with honesty and integrity ▪ Treat people with care and compassion	▪ Support the needs of each individual ▪ Encourage personal development and independence ▪ Provide safety, stability and security
Responsibility	**Excellence**
▪ Work together, in partnership ▪ Take responsibility for our actions ▪ Continue learning and improving	▪ Provide a first-class service ▪ Deliver excellent value for money ▪ Explore innovative ways of working

Contents

1. Introduction

1.1 We have produced this policy and its supporting documents detailing and regulating the use of CCTV across Transform. This policy forms part of Transform's information governance framework.

1.2 This CCTV Policy applies to all CCTV installations owned, approved or operated by us. It applies to all footage captured by these installations and to those people responsible for or operating any of our CCTV installations (employees, volunteers, contractors etc).

1.3 This Policy will be shared to key staff groups as below:

- Directors – communication directly by email and discussion at Executive Team Meeting
- Senior Leadership Team
- Key Policy users – through the Operational Managers
- All staff – through MILO - all new starters will be made aware of this Policy as part of their induction process. Managers will be responsible for keeping staff up to date with any changes to this Policy.

2. Definitions

2.1 The Definitions used in this policy have the meanings attributed to them in the UKGDPR and the Data Protection Act 2018.

2.2 The following types of CCTV installation are within the scope of this policy. At time of writing this policy, we only have overt CCTV.

Overt CCTV

2.3 Generally defined as permanent or temporary cameras that are obvious and would be reasonably expected to be in situ e.g., security cameras on the exterior of buildings.

Covert CCTV

2.4 Generally defined as cameras that are not obvious or are hidden including:

- Cameras embedded in other equipment such as smoke detectors, glasses (including Google Glasses), watches, street furniture, PPE, pens, badges etc.
- Cameras that are deliberately hidden to avoid detection
- Cameras that may not be obvious or obviously collecting footage such as drones dashcams, Go Pros and similar small cameras that whilst not hidden are not obvious, body worn cams which may not be obvious to those being filmed
- Cameras used on mobile phones where their use is not obvious.

Excluded cameras

2.5 Vehicle reversing aids when there is no recording of images; broadcast video cameras used for broadcasting or collecting footage for promotional purposes such as corporate videos, training videos etc. **are excluded** from this CCTV policy.

3. Guidance and Legislation

3.1 The Data Protection Act 2018 (DPA18) and UK General Data Protection Regulation (UKGDPR) 2021 set out a legally binding framework that we and any contractors must comply with.

3.2 Transform, its contractors and colleagues will be held accountable for failure to comply with the law and may be subject to regulatory action including fines and other enforcement actions.

4. Roles and Responsibilities

4.1 **The Chief Executive** is responsible for ensuring that all our data processing activities comply with the law and the best practices set out in its policies and procedures.

4.2 **The Head of Governance & Assurance** is responsible for defining work practices that are compliant with the law and best practices through establishing policies and procedures and ensuring that they are made available to all relevant people. They are responsible for monitoring all CCTV installations from their inception through their installation, operation and management and eventual decommissioning.

4.3 **The Head of Digital & Information Services** is responsible for ensuring that all information including video footage, still images, and audio recordings is captured, transmitted, and stored securely in line with the Data Protection policy and Data Protection Impact Assessment.

4.4 They will ensure that all operational managers are provided with clear guidance, briefing materials and training on the operation of the equipment, including identifying relevant footage and downloading it securely.

4.5 **The Heads of Housing & Support** are considered **Information asset owners** and are responsible for:

- Undertaking Data Protection Impact Assessments (DPIA) in accordance with the Data Protection Policy using the DPIA form

4.6 The **Housing & Support Managers** are the **CCTV managers**

- Ensuring the security of CCTV equipment under their responsibility and for complying with this policy and related documentation
- Assisting the Head of Digital & Information Services in ensuring the security of the information collected/captured by CCTV equipment they are responsible for
- Ensuring that the CCTV equipment they are responsible for is operating in compliance with this policy and related documents

4.7 All colleagues are responsible for reading, ensuring a full understanding of and complying with this policy and related procedures and instructions. All employees are responsible for reporting to the **Head of Governance & Assurance** any non-compliance that they are aware of or suspect.

5. PROCEDURES

Overview

5.1 We will only use CCTV where it is a proportionate and necessary measure to achieve a defined business objective.

5.2 We use overt CCTV systems and would not use covert CCTV systems unless approved by the Executive or by an emergency decision by the **Chief Executive** and only in exceptional circumstances.

5.3 CCTV installations will only be commissioned or deployed in accordance with this policy and related work instructions and procedures.

5.4 Prior to deploying CCTV, a Data Protection Impact Assessment (DPIA) will be undertaken by the Head of Housing & Support wishing to introduce the CCTV in accordance with the DPIA procedures.

5.5 A register shall be maintained by the Head of Governance & Assurance of all installations of CCTV of which we are either a Data Controller or a Data Processor.

5.6 All approved CCTV installations shall have a defined manager, usually the local Housing and Support Manager.

5.7 When no longer needed CCTV installations shall be subject to a decommissioning procedure (see Section 14).

5.8 Failure to comply with this policy and related procedures and jeopardising our integrity and compliance with the law will be addressed under our disciplinary procedures

6. Commissioning a New CCTV installation

6.1 The following process shall be followed by the individual wishing to introduce a CCTV. Where there is a need for a new CCTV installation a CCTV request form should be completed

Tendering

6.2 Competitive tenders will be sought where necessary in accordance with our Procurement Policy

Technical specifications

6.3 The technical specification of CCTV systems will be defined in writing and such that the resulting images collected are of sufficient quality to satisfy the purpose of the installation, allow for appropriate access control of recorded images, and collect no more information than is needed to satisfy the purposes of the installation.

Data Protection Impact Assessment (DPIA)

6.4 A DPIA will be undertaken for all proposed CCTV installations or use. This will ensure there is a thorough and objective critical analysis of the legitimacy and need for the CCTV being proposed and to uncover, highlight and mitigate any potential risks to the privacy, rights, and freedoms of individuals. This will ensure that the measures being implemented are appropriate and that an adequate level of due diligence has been completed.

6.5 CCTV installations in situ shall be subject to a DPIA review periodically (at least annually) by the Head of Housing & Support. The CCTV DPIA review period shall be recorded in the Register of CCTV Installations.

6.6 The person requesting to install the CCTV will be responsible for undertaking the CCTV DPIA with support from the Head of Governance & Assurance.

6.7 CCTV DPIAs shall be recorded on a CCTV DPIA form found on MILO.

6.8 CCTV DPIAs shall be approved by the Executive Team. The external Data Protection Officer will also be involved in reviewing the DPIA.

Lawful grounds

6.9 CCTV recordings will be used for our legitimate interest such as the prevention and detection of anti-social behaviour and crime, safeguarding staff and visitors, ensuring compliance with health and safety procedures, the apprehension and prosecution of offenders (including the use of images as evidence in criminal proceedings) and ensuring compliance with the Code of Conduct. Footage should only be viewed when an incident has taken place that necessitates this.

Approval

6.10 No CCTV installations shall be commissioned or installed unless a DPIA and business case has been completed and approved by the Executive Team in accordance with this procedure. Any installations will need to be financially viable with any charges recovered through the service charge setting process as per the rent and charge setting policy.

6.11 There may be justification to bypass formal approval processes in rare and unusual situations such as an emergency or a safeguarding concern. Approval of the **Chief Executive** should be sought and formal approval processes must be followed up as soon as possible afterwards. The **Chief Executive** or his Deputy should approve the bypassing of formal approval processes and report to the next meeting of the Board of Trustees

Installation

6.12 An approved contractor identified by the Head of Digital & Information Systems shall be used to install the CCTV equipment in accordance with the required standards and in line with the NCP 104 providing details, recommendations and guidance as part of a CCTV system design and ensures sustainability, functionality and effectiveness of a system. The Code is in line with the latest standard BS EN 62676-4:2015. All cameras installed must be a minimum standard of 5 Mega Pixels.

Commissioning

6.13 All CCTV installations shall be subject to a commissioning process to be undertaken by the **Information Asset Owner** which shall include:

- Checking that the installation is precisely as detailed in the DPIA or that a variation to the DPIA has been approved
- Checking that cameras, cables, transmission equipment and data storage are tamper-proof
- Collecting and retaining still images of the field of view of each camera for use as a future field of view reference point
- Checking and verifying that the access controls defined in the DPIA are in place and are effective
- Checking and verifying that the data retention policy defined in the DPIA is effective

- Ensuring appropriate signage is erected as detailed in the DPIA
- Checking that relevant information has been recorded on the Register of CCTV installations held by the **Head of Governance & Assurance**.
- The **Information Asset Owner** will certify that the CCTV installation complies with these requirements

7. Commissioning Additional Camera(s) for an existing CCTV system

7.1 A CCTV request form should be completed. The request should be approved by an Information Asset Owner in consultation with the Head of Governance & Assurance and or the Data Protection Officer. The relevant DPIA will need to be updated accordingly.

8. Assuming responsibility for a property with existing CCTV system

8.1 A DPIA should be completed for the system (unless one already exists) and this should be approved in the same way as commissioning a new system.

9. Privacy Information

9.1 Where required, privacy information shall be displayed prominently to ensure that people are made aware of the use of CCTV before they enter and whilst they are at any of our sites.

9.2 The **Head of Governance & Assurance** shall be responsible for creating appropriate privacy information. **Information Asset Owners** and **CCTV Managers** will ensure that this is installed as part of the commissioning process set out in 6.13 above.

9.3 We will adopt a tiered approach as detailed below, to providing privacy information relating to CCTV installations.

9.4 The most important information shall be displayed on the warning sign, which is the first layer, and further mandatory information on the second layer.

First layer

9.5 The warning sign will be provided in combination with an icon (such as a picture of a surveillance camera). The information shall be positioned in such a way that the data subject can easily recognise that there is CCTV before entering the monitored area. This layer shall convey the most important information e.g., details of the purposes of processing, the identity of the data controller and the existence of data subject rights, together with information on the greatest impacts of the processing.

9.6 Our privacy notice provides additional privacy information. First layer privacy information shall as a minimum include:

- A warning that CCTV is in operation
- The name of the data controller (i.e., Transform Housing & Support)
- The purpose of the CCTV installation and lawful basis of the data processing
- Contact details of the Head of Governance & Assurance
- Telephone number and email address.

Second layer

9.7 This layer (containing all information under Article 13 GDPR) will be available at an easily accessible place in the local office or displayed on an easily accessible poster. It is best if the first layer refers to a digital source (e.g., QR-code or a website address).

9.8 The **Information Asset Owner** shall ensure the installation of appropriate privacy information in liaison with the **Head of Governance & Assurance**, asset management colleagues and or CCTV installation companies. This is an example:

9.9 The inclusion of this wording on signage for overt CCTV will ensure that data subjects are sufficiently informed in accordance with the GDPR.

Privacy information and covert CCTV

9.10 Appropriate privacy information shall be made available in the case of covert CCTV operations unless an exemption applies in the specific situation. Schedule 2, 3 and 4 of the Data Protection Act 2018 contain exemptions to the requirement to provide privacy information. The **Head of Governance & Assurance** shall ensure there is a written justification for all instances of CCTV implementations where privacy information is not provided. Transform may undertake or permit the relevant authorities to undertake covert CCTV operations without specifically notifying individuals where illegal activities are occurring (see 16.3).

10. Operating CCTV installations

Data Retention and Storage

10.1 Due to the potentially sensitive nature of CCTV images we will employ strict retention periods and storage rules to the storage of CCTV footage in line with its data retention policy.

10.2 Transform shall ensure that, by default, CCTV images are retained for **no longer than 30 days** unless images are required for an investigation such as a police investigation or an investigation taking place under our disciplinary procedures. Footage should only be viewed when an incident has taken place that necessitates this.

10.3 Images required for a police investigation shall be removed from the CCTV storage system and stored in a relevant folder within **the CCTV and other information requests** channel of the **Data Subject Access Requests team**

10.4 Images required for an investigation shall be retained for no longer than a period of 2 years following the end of the investigation as advised by our Data Protection Officer.

10.5 The **Head of Governance & Assurance** shall maintain a register of CCTV images stored for investigation.

10.6 The **Information Asset Owner**, in consultation with the **Head of Governance & Assurance**, shall reassess any CCTV images retained for investigation which have reached the end of their retention period to decide whether they are required to be retained any longer.

10.7CCTV images shall be stored in such a way as to ensure confidentiality integrity, availability and restorability. CCTV storage locations shall be approved by the **Head of Digital & Information Services**.

11. Erasure

11.1 CCTV footage reaching the end of its retention period will be automatically deleted by the CCTV system.

11.2 The **Head of Digital & Information Services** shall define what measures are appropriate to destroy CCTV images.

11.3 CCTV images retained for other purposes shall be anonymised using an appropriate technical measure such as those advised by the EDPB (for example the scrambling or pixelation of individuals' faces in CCTV footage to the extent that the modification renders the modified images beyond recovery and the individuals can in no way be identified or are identifiable).

11.4 The **Information Asset Owner**, in consultation with **the Head of Governance & Assurance**, shall review all CCTV images that are re-purposed and approve them for use. Modified CCTV images that have not been approved by the Data Protection Lead shall be prohibited from use.

Measures to ensure the security of CCTV images

11.5 The **Head of Digital & Information Services** shall ensure that all CCTV images are adequately protected from accidental or unlawful destruction, loss, or alteration. Arrangements for access are defined in the CCTV Access and Permissions Policy.

11.6 The systems used to collect, transmit, store, and otherwise process CCTV footage are subject to the same high standards of IT security which run throughout the entirety of Transform, including access controls, user authentication, anti-virus and malware software, penetration testing etc

Viewing recorded CCTV Images

11.7 Recorded CCTV images shall only be reviewed as authorised by the **Information Asset Owner**, in consultation with the **Head of Governance & Assurance** where there is a defined business need.

11.8 Requests to review recorded CCTV images shall be submitted to the **Head of Governance & Assurance** for logging a record should be kept of the request should be maintained to ensure recordings are being viewed for legitimate purposes, Data Subject Access Request processes should also be followed.

11.9 The viewing of recorded CCTV images shall take place in a restricted area co-ordinated by a nominated colleague as identified by the **Information Asset Owner**, for example, in a designated member of staff's office. Other parties should not be allowed to have access when a viewing is taking place.

11.10 Recorded CCTV images shall not be retained by the viewer once the viewing is concluded. The **Information Asset Owner** will ensure that all means of access to the images are removed after the viewing.

12. Viewing live CCTV images

120.1 Transform shall ensure that any CCTV images that are available for live viewing shall not be capable of allowing the monitoring of people's behaviour unless this is the specific purpose of the installation (e.g. car park surveillance, fly tipping etc.).

12.2 The live feed for CCTV images that are specifically implemented for the purpose of monitoring behaviour shall terminate in a secure area with access limited to specific designated personnel and the live feed channels are not on display or viewed by unauthorised personnel e.g. located in secure office spaces.

13. Disclosure of CCTV Images

13.1 We receive requests for the disclosure of CCTV footage from time to time from organisations such as the police.

13.2 All colleagues receiving such a request shall pass the request to the **Head of Governance & Assurance.**

13.3 The **Head of Governance & Assurance** shall ensure that a register or all requests for CCTV footage disclosure is maintained. Details of requests must be entered on the **register of information requests**. All supporting correspondence and footage will be saved to the relevant folder within **the CCTV and other information requests** channel of the CCTV and other information request channel of the **Data Subject Access Requests team.** Access to the folder will be limited to the **Head of Governance & Assurance**, **Data and Performance Manager**, **Head of Digital & Information Services**, the **CCTV Manager** and the **Information Asset Owner**

13.4 The **Head of Governance & Assurance** shall assess each disclosure request on its merits and shall always exercise the highest degree of scrutiny and caution to ensure the privacy of people who feature on the footage is not compromised. In assessing each request for disclosure, the **Head of Governance & Assurance**, in consultation with the **Information Asset Owner** shall consider:

- The purpose of the request, aim of the requestor and proposed use of the requested footage.

- Our lawful grounds for disclosure.
- The rights of individuals which may favour non-disclosure.
- The necessity of the disclosure to further the requestors' purpose.

13.5 Requests for disclosure shall always be made in writing/via email to support verbal requests.

13.6 Request from organisations such as the Police are likely to be subject to the requesting organisation's policy such as approved by senior management. After considering all factors associated with the request, the **Head of Governance & Assurance** shall decide whether the footage should be disclosed and any terms relating to the disclosure.

13.7 The **Head of Governance & Assurance** shall ensure that the register of disclosure requests contains sufficient information regarding how the request was handled.

14. Maintenance

14.1 CCTV installations shall be subject to a structured schedule for routine maintenance undertaken by an appropriately qualified contractor. A maintenance contract must be entered into for all CCTV installations. Servicing dates for CCTV will be held on Pyramid and reminders given to the Head if Digital and Information Systems.

15. Compliance checking

15.1 The CCTV Manager will verify the compliance of the CCTV installation to this policy and report accordingly:

- Quarterly
  - still to live image check
  - data retention check
  - privacy information check
- Annual re-evaluation of the need (in line with DPIA findings)
- Annual check of maintenance records
- A record of the checks will be completed, and the results shared with the Information Asset Owner

16. Decommissioning

16.1 When CCTV systems are no longer needed and agreed by a senior manager, they shall be subject to a decommissioning procedure that includes:

- Removal of equipment
- Destruction of images
- Removal of signage

17. Lawfulness of Processing

17.1 As with all instances where personal data is processed there must be lawful basis for doing so in line with the UKGDPR. As CCTV has the added risk of monitoring individuals it is crucial that we adopt an appropriate lawful basis for all its CCTV installations.

17.2 We will be processing personal data through the medium of CCTV installations aswe have both a legitimate interest in doing so and will be carrying out a task which is in the public interest in the process.

17.3 We have a legitimate interest in ensuring the safety of our premises and detecting and preventing any unlawful acts which may take place on our premises. Additionally, we have a legitimate interest in monitoring our colleagues and clients to ensure their health and safety, safeguarding and compliance with the Code of Conduct.

17.4 In processing personal data through the medium of CCTV installations we are s carrying out a task in the public interest, namely the detection and prevention of unlawful acts as defined in the Data Protection Act 2018 (DPA) schedule 1 part 2 section 10.

18. Processing of special categories of personal data

18.1 The European Data Protection Board (EDPB) has published guidelines on the usage of CCTV. In the context of special categories of personal data, they have stated that CCTV will not be capturing special category data by default unless it has specifically installed to monitor such data.

18.2 Transform will not install any CCTV which actively monitors special categories of personal data such as the monitoring of computer terminals.

Covert CCTV in the workplace

18.3 We will not normally use covert CCTV in the workplace.We will only approve such covert use if we are satisfied that there are grounds for suspecting criminal activity or equivalent malpractice. In such cases, individuals will not be specifically notified about the use of covert CCTV as this may be prejudicial to the prevention or detection of crime or the outcome of an official investigation. Any use of covert CCTV should be signed off by the Chief Executive and identified within the wider Employee Privacy Notice.

Use of video recording by others

18.4 The use of video recording equipment (including mobile phones) on our premises shall be prohibited unless specifically authorised by the Head of Housing & Support If a member of staff is found to have inappropriately made a recording, retained or shared a recording then this may lead to disciplinary procedures.

18.5 Clients who are tenants and have exclusive possession of their home, will be provided with advice on their legal responsibilities should they wish to install devices such as camera doorbells or internal cameras. This advice will be provided retrospectively where colleagues become aware that such devices have been installed. Where such devices interfere with other client's or neighbours' peaceful enjoyment of their properties, this will be dealt with through support, mediation and ultimately under our ASB policy and procedure. Clients will not be permitted to mount CCTV or other recording devices on the outside of Transform properties or in internal or external shared and communal areas.

19. Data Subject Rights

19.1 As a controller of personal data all the rights afforded to data subjects under the UKGDPR will apply to our use of CCTV. More details on subject rights and the timescales for processing these are set out in the Data Protection Policy In relation to this specific activity the EDPB has provided some added clarification for some of the data subject's rights as follows:

Access rights

19.2 Complying with access rights in relation to video surveillance could adversely affect the rights of other data subjects who are also identifiable from the footage. Image editing and scrambling shall be used to protect these third parties. We may also ask the data subject to specify reasonable timeframes to help with information searches.

Right to erasure

19.3`The EDPB notes that blurring a picture with no retrospective ability to re-convert the picture into an identifiable image constitutes erasure in accordance with GDPR.

Right to object

197.4 In case of video surveillance, this right could be exercised either prior to entering, during the time in, or after leaving the monitored area. This means that unless the controller has compelling legitimate grounds, monitoring an area where persons could be identified is only lawful if either: (1) the controller is able to immediately stop the camera from processing personal data when requested, or (2) the monitored area restricted so that the controller can assure the approval from the data subject prior to entering.

20. Monitoring and Review

Policy Review Cycle

20.1 This policy is subject to a **three yearly** review. Transform will undertake a formal review of this policy by no later than three years from the date shown above, or earlier, if significant changes and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.