CCTV Policy

Policy Owner:	Data Protection Officer (Executive Director: Finance)
Policy Lead:	Governance Manager
Approved by:	Executive Team
Approved date:	January 2025
Next review date:	January 2026

Contents

Purpose and scope of the policy

Purpose

The purpose of this policy is to ensure that our use of CCTV complies with the UK General Data Protection Regulations (UKGDPR) and associated legislation and codes of practice, in particular the 12 principles of the Surveillance Camera Commissioner's Code of Practice, which are set out in the policy under the following headings.

- Specific Purpose
- Data Privacy Impact Assessment (DPIA)
- Transparency
- Responsibility and accountability
- Policies and procedures
- Data security, storage and retention
- Access management
- Technical standards
- Review, audit and monitoring
- Third party suppliers
- Complaints

Scope

This policy applies to:

- all colleagues involved in the procurement and/or implementation of systems, overseeing operational maintenance, reviewing and retrieving recorded activity.
- external suppliers who supply, maintain, operate and remove CCTV systems on our behalf.
- all sites, offices owned/managed/leased by Moat and any other land, asset or property that Moat control where CCTV is already implemented and sites where CCTV is proposed for implementation.
- Moat's use of overt and covert CCTV both fixed and deployable.
- the rapid deployment of covert cameras on request of the Police or other authority.

This policy does not apply to:

- the maintenance, operation and installation of CCTV in offices and locations which are not owned, managed, or leased by Moat.

- domestic systems which are not deployed by Moat e.g. CCTV systems installed by customers to monitor their own properties.
- Ongoing monitoring and consistent surveillance of footage at any location.

Roles and Responsibilities

Neighbourhoods, Building Safety, Facilities, Development, Data and Technology, Procurement and Governance:
The Director(s) and Manager(s) responsible for CCTV must make sure that the mechanisms set out in this policy are implemented through their management structures and that staff are aware of the requirements of this policy.

All Colleagues:

All colleagues must comply with this policy and report any concerns or incidents relating to CCTV and its use to their line manager. These reports must then be passed immediately to the Data Protection Officer, where such reports identify a potential breach of the UKGDPR.

Any colleague can receive a request for CCTV footage and should therefore be aware of the content of this policy and associated procedure.
All colleagues should be aware of their roles and responsibilities under this policy and associated procedure, and be up to date with their training requirements.

Data Protection Officer (DPO)

- Develop CCTV and associated data security policies.
- Ensure Moat's compliance with this policy and related legislation.
- Approve Moat's CCTV data protection impact assessment (DPIA), monitor associated risk mitigations and conduct annual reviews.
- Ensure that appropriate and up to date training is in place.
- Ensure that processes are in place to undertake regular audits on all records relating to our CCTV systems to ensure that the policy is being adhered to.
- Set the retention period to be adhered to on the recording device, as well as footage that has been extracted for a specified purpose that is to be stored outside of the recording device.

Director of Neighbourhoods (for any cameras installed and maintained within their service area)

- Ensure compliance with this policy, procedure and related legislation within the Directorate.
- Monitor the Directorate's compliance with ongoing training requirements.
- Agree, monitor and control authorised access levels to footage.
- Authorise requests for rapid deployment and covert cameras.

Director of Development, Director of Communications and Facilities (for any cameras installed and maintained within their service area)

- Ensure compliance with this policy, procedure and related legislation within the Directorate.
- Monitor the Directorate's compliance with ongoing training requirements.
- Agree, monitor and control authorised access levels to footage.

Neighbourhood Services Managers and Tenancy Specialist Team (for residential areas owned and managed by Moat),
Facilities Manager (for Moat offices):

- Ensure that the centrally maintained register of CCTV systems is accurate and up to date.
- Annually review the DPIA and business case for CCTV in each location.
- Process any request for accessing/viewing/extracting/securing/sharing footage in line with the associated CCTV procedure.
- Where the retention period has expired, delete footage in line with the Data Retention Schedule.
- Handle complaints about the CCTV system.

Building Safety Manager – CCTV Third Party Contract Manager,
Facilities Manager (for Moat offices),
Development Project Manager (for land under development):

- Ensure the CCTV and Door Entry Systems are technically operational and that footage is of a reasonable quality for the intended purpose(s).
- Ensure that cameras and associated devices are installed or deployed in accordance with Building Safety, Data Protection regulations and Surveillance Camera Commissioner's Technical Standards.
- Oversee the management of the third-party organisation responsible for maintenance of cameras and recording equipment and retrieval of associated footage.
- Ensure that the centrally maintained register of CCTV systems is accurate and up to date.
- Procure CCTV and Door Entry systems in accordance with Moat's Procurement Policy, Data Protection Policy, Data and Technology Policies and Surveillance Camera Commissioner's Technical Standards.
- In conjunction with Procurement, Governance, and Data and Technology, complete a data protection impact assessment (DPIA) on every new proposed, or change to existing, cameras, recording equipment, software and access levels.
- Annually review the DPIA and business case for CCTV in each location to ensure that the visual recording system is justified and that the devices used are appropriate for the purpose(s) specified.
- Propose authorised access levels to footage for authorisation.
- Complete electronic logs to evidence incidents (door entry systems)
- Process any request for accessing/viewing/extracting/securing/sharing footage in line with the associated CCTV procedure.

Data and Technology

- In conjunction with all stakeholders, complete a data protection impact assessment (DPIA) on every new proposed, or change to existing, cameras, recording equipment, software and access, approving CCTV systems hardware and software for use before installation.
- Ensure that appropriate minimum standards are set in relation to technologies associated with CCTV, in particular their security measures and data storage and transfer methods.

Data Protection Coordinator

- Authorise the disclosure of requests for CCTV footage.
- Maintain a register of all active CCTV systems at all locations, including their technological specifications and a list of authorised users.
- Undertake annual audits on all records relating to our CCTV systems including recording of requests, asset lists and granting of access rights to ensure that the policy is being adhered to.

CCTV System Operator and its operatives (third-party service providers)

- Carry out CCTV installations upon request and provide CCTV Operational Guidelines.
- Ensure that systems are installed in compliance with this policy and minimum system requirements.
- Access/view/extract/secure/share CCTV footage in response to authorised requests in line with this policy.
- Ensure compliance with the Contractor's Code of Conduct, particularly when undertaking visits to site on request.
- Ensure that access is provided in accordance with approved and up to date user lists.

1. Specific Purpose

1.1. We operate a number of closed-circuit television (CCTV) systems and in so doing aim to:

- safeguard the health, safety and security of customers, colleagues and other users of our buildings, communal areas and open spaces where we have a controlling interest.
- protect the asset value of those buildings we own and control by deterring/preventing crime such as vandalism or theft.
- assist in the prevention of crime, anti-social behaviour, public order offences and other statutory enforcement issues by providing information to relevant authorities to enable them to take enforcement action.

1.2. Any CCTV in our control and operation must be in line with the above purpose(s).

1.3. We have determined the lawful basis for processing information captured and recorded on CCTV systems in our control and operation as: in accordance with the UK General Data Protection Act (UKGDPR) Schedule 1 "Substantial Public

Interest", Paragraph (10) "preventing or detecting unlawful acts". Any CCTV use or operation which does not comply with this purpose(s) is strictly prohibited.

1.4. These purposes will be outlined within our Privacy Statement available on our website. Any changes to the purpose(s) for which we are operating CCTV will initiate a revision of our Privacy Statement and CCTV Policy and Procedure.

1.5. Any unauthorised use or operation of CCTV and associated footage will be addressed in line with our Disciplinary Policy.

1.6. We will only capture what we need to for the agreed purpose(s). Camera positioning will be directed to general public / communal areas, not at individual residential addresses and/or property. We will not use audio, facial recognition technologies or biometric characteristic recognition.

2. Transparency

2.1. We will ensure that we are transparent in the use of CCTV by placing signage at all overt CCTV locations which will detail:

- the organisation operating the system and contact information.
- location of our Privacy Statement setting out our lawful basis for processing in accordance with Article 5(1)(a) of the UKGDPR.
- why the system is in operation (the purpose(s)).

2.2. We may need to install covert cameras where required for building evidence in serious cases of breaches of tenancy (or other) agreement or public safety. We'll only do this on an exceptional basis where there are no other options for remedy, i.e. members of the public or neighbours are not willing to provide witness statements due to concern for their personal safety.

3. Responsibility and accountability

3.1. This policy sets out clear responsibilities and accountabilities for all CCTV activities, including management and operational roles, and how we properly manage any data processed in association with CCTV.

4. Policies and procedures

4.1. Along with this policy we will have a procedure in place to cover:

- new CCTV installations
- third-party disclosures by Moat

4.2. We will maintain accurate and up to date records relating to our CCTV systems including:

- recording of requests for access to footage and our decision.
- asset lists for each CCTV system in operation including location, technological specification and access.
- granting of access rights.

- annual audits to ensure that the policy is being adhered to.

5. Data security, storage and retention

5.1. We will not capture and/or store footage or images other than that which is strictly required for the stated purpose(s) of the CCTV, and such footage or images will be deleted in line with our data retention schedule.

5.2. Footage held within the visual recording system will be stored for 30 days, after which time, the footage will be automatically destroyed.

5.3. Any footage downloaded and stored outside of the recording system will be stored until the evidence is no longer required for the purposes of the legal proceedings, and then destroyed in line with our data retention schedule.

5.4. All footage in the visual recording system and any isolated/extracted footage will be retained in a secure environment e.g. stored on a restricted access network drive and encrypted. Any online/cloud-based storage or transfer of data from the recording system to the storage system will also be secure and encrypted.

6. Access Management

6.1. Access to recording systems and CCTV footage will be controlled so as to only allow those with an agreed purpose(s) and objective and will be by authorisation only.

6.2. The disclosure of images and information will only take place when it is necessary for such lawful purpose(s) and will be authorised.

6.3. Access to footage by customers, members of the public or colleagues will not be provided where the information includes the personal data of other third-parties (i.e. it is about another party or property) or is about an incident which does not directly involve them. In these cases (e.g. theft of property or ASB) a request must be made by the appropriate authorised third party (e.g. police).

7. Technical standards

7.1. Any CCTV recording system that we procure will meet the technical requirements as set in the Surveillance Camera Commissioner's Technical Standards and/or other industry standards, in particular BS EN 62676 Video Surveillance Systems requirements.

7.2. We must meet the Cyber Essentials+ standard requirements and will only engage potential suppliers that can demonstrate that they meet the same criteria.

7.3. In all cases, footage will be legible, fit for purpose and captured and stored in a resolution sufficient to allow the footage to be used for evidential purposes and

the purposes set out in the Data Privacy Impact Assessment (DPIA) and approved business case.

7.4. Cloud-based storage and transfer will be restricted to the UK and offer sufficient security. Any instances where there is the possibility for international data transfers would trigger a Data Transfer Agreement, update of the Privacy Statement and Register of Processing Activities.

8. Review, audit and monitoring

8.1. We will have effective review and auditing mechanisms to ensure:

- we meet our legal requirements.
- all business cases (including appended checklist and DPIA) for all CCTV systems are reviewed annually.
- we comply with our policies and standards in practice.

8.2. Regular audits will be carried out on all records relating to our CCTV systems including recording of requests, asset lists and granting of access rights to ensure that the policy is being adhered to.

9. Camera location

9.1. We will not install cameras in areas which are considered as private, such as in toilets, changing rooms or directed towards an individual's property (so as to single them out). Cameras installed must be directed towards public spaces, which must make up at least 80% of the viewable image. The viewable image must not allow the inside of a customer's home to be seen (i.e. doors and windows).

9.2. In exceptional cases, such as when dealing with repeated serious antisocial behaviour, it may be necessary to have surveillance in private areas; this will be carefully considered on a case-by-case basis.

9.3. Customers requesting to install their own CCTV systems, including video doorbells, must ask for, and receive, written permission; and be directed towards the ICO's guidance on home CCTV systems.

10. Third party suppliers

10.1. Where CCTV is provided by third party suppliers, we will ensure that they adhere to this policy with regard to technical standards, access management and retention of footage.

10.2. Contracts with suppliers must also stipulate the service level agreements for returning footage in response to requests to ensure that legal obligations in respect of subject access and third-party requests can be met within the appropriate timescales. Third-party suppliers are approved and authorised in line

with our Procurement Policy and in line with the Surveillance Camera Commissioner's Buyer's Toolkit when specifying system requirements.

10.3. Service providers will demonstrate that computing systems in operation are compliant with our Data and Technology Security Policy and will have cybersecurity certifications appropriate for their use (such as ISO 27001).

10.4. The technology in use must be explored to understand whether sharing of personal data might amount to an internation data transfer, which would trigger a Data Transfer Agreement.

11. Complaints

11.1. Where a complaint is received regarding the use of a visual recording system from a member of the public or an authorised representative (e.g. MP, Councillor, solicitor etc.) this will be handled in accordance with our Complaints Policy.

Definitions
• **BS EN 62676** – As defined by the British Standard. • **CCTV** – Closed Circuit Television. S29(6) of the Protection of Freedoms Act 2012 (PoFA) states that "surveillance camera systems" mean: (a) closed circuit television or automatic number plate recognition systems, (b) any other systems for recording or viewing visual images for surveillance purposes, (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c). • **Covert** - not openly acknowledged or displayed (usually requested by the Police when ongoing crime has been identified and in line with our ASB Policy). • **Data controller** – As defined in the UKGDPR. • **Data Privacy Impact Assessment (DPIA)** – As defined in the UKGDPR. • **Data Protection Officer (DPO**) – As defined in the UKGDPR. • **Data Subject Access Request (DSAR)** – As defined in the UKGDPR. • **MP** – Member of Parliament. • **Overt** - done or shown openly; plainly apparent (the majority of our CCTV systems will be defined this way). • **Register of Processing Activities** – As defined in the UKGDPR. • **UKGDPR** – UK General Data Protection Regulations.

Equality, Diversity and Inclusion
This policy will be delivered in accordance with our Equality, Diversity and Inclusion Policy. An Equality Impact Assessment was completed for this policy and considered as part of the approval process.

Data protection

This policy will be delivered in accordance with our Data Protection Policy.
A Data Impact Assessment was completed for this policy and considered as part of the approval process.

Related legislation and regulations

- Human Rights Act 1998
- UK General Data Protection Regulations (UK GDPR) 2018
- Protection of Freedoms Act 2012
- Surveillance Camera Commissioner's Code of Practice
- British Standard BS EN 62676

Related policies and procedures

- Antisocial Behaviour Policy
- CCTV Procedure
- Complaints Policy
- Data Protection Policy
- Data and Technology Security Policy
- Data and Technology Third Party Access Policy
- Data and Technology Acceptable Use Policy
- Data and Technology Software Standards Policy
- Disciplinary Policy and Procedure
- Domestic Abuse Policy (Colleagues)
- Domestic Abuse Policy (Customers)
- Equality, Diversity and Inclusion Policy
- Hate Related Incidents Policy
- Health and Safety Management Policy
- Home Adaptations Policy
- Neighbourhood Management Policy
- Procurement Framework (including Contractor's Code of Conduct)
- Safeguarding Adults at Risk Policy
- Safeguarding Children Policy
- Tenancy Fraud Policy
- Tenancy Management Policy

Customer engagement

This policy has been shared with our Customer Advocate group. 17 customers reviewed the policy and all customers but one confirmed that they found the policy clear and easy to understand, and that they support the adoption of the policy, with no amendments suggested.

Document Revision History (Record of any changes made to the policy)		
Date	**Changes approved by**	**Details of changes made**