

CCTV and Audio Recording Policy

Document Owner	Head of Governance, Risk and Assurance
Prepared by	Policy Officer and Data Protection Officer
Approved by	Directors Group
Approved date	August 2024
Date of next review	August 2027
Monitoring, Auditing and Reporting	See section 8 of this Policy

1 Scope and Aims

- 1.1 This policy applies to the use of overt closed circuit television (CCTV), surveillance cameras and audio recording equipment by, or on behalf of, Hexagon.
- 1.2 The policy applies to CCTV used by Hexagon or by agencies operating within Hexagon owned schemes. This Policy applies to, and must be complied with by, all employees (whether temporary or permanent), workers, contractors, agents, representatives and other third parties (referred to collectively as 'colleagues') acting for or on behalf of Hexagon.
- 1.3 Hexagon does not use covert CCTV equipment, so its use will not be sanctioned within this policy.
- 1.4 Hexagon will use CCTV to prevent and detect anti-social behaviour, prevent and detect tenancy fraud and property damage, provide safety mitigations, and crime prevention in and around some of our properties which we own or manage, our offices, car parks and communal areas where there is an assessed risk, and to help safeguard residents, colleagues and visitors to those properties and on our land.

2 Equality and Diversity

- 2.1 Hexagon will ensure that this policy is applied fairly and consistently and will not directly or indirectly discriminate against any person or group in line with equality law and principles. We will act sensitively towards the diverse needs of individuals and communities and will take positive action where appropriate.
- 2.2 An equality impact assessment 'initial screening' (Appendix 1) has been carried out which determined there to be no negative impact specific to those with protected characteristics.

3 Policy Statement

- 3.1 Hexagon takes its obligations in relation to the protection of personal data seriously.
- 3.2 CCTV can provide significant security benefits and is particularly useful in high-risk areas. Similarly, audio recording is often essential evidence in noise nuisance cases.

- 3.3 Both formats have the potential to record sensitive personal data. We want to make sure we use CCTV and audio recording effectively, with clear purpose and in a way that minimises the unnecessary sharing of personal data.
- 3.4 CCTV installations shall only be commissioned or deployed in accordance with this policy and related work instructions and procedures.
- 3.5 Prior to any deployment of CCTV a Data Protection Impact Assessment (DPIA) shall be undertaken by Hexagon.
- 3.6 A record shall be maintained of all deployments of CCTV of which Hexagon is either a Data Controller or a Data Processor.
- 3.7 All approved CCTV installations shall have a defined owner. A register of information assets and their owners shall be maintained by Hexagon in accordance with the Data Protection Policy.
- 3.8 When no longer needed CCTV installations shall be subject to a decommissioning procedure.

4 Objectives

- 4.1 This Policy aims to ensure that CCTV on our premises is operated to enhance safety, and the sense of safety; and thereby assists in encouraging use of our facilities, through the following objectives:
 - 4.1.1 To assist in deterring crime and assist in the detection of criminal offences;
 - 4.1.2 To assist in the detection of criminal offences, anti-social behaviour incidents and to provide evidence for court proceedings;
 - 4.1.3 Reducing the fear of crime and anti-social behaviour for residents and colleagues;
 - 4.1.4 Improving the safety and security of residents and visitors;
 - 4.1.5 To assist in the investigation of health and safety incidents and the review of health and safety management;
 - 4.1.6 To support HR disciplinary processes where gross misconduct is alleged.
- 4.2 This Policy aims to ensure that CCTV is used transparently, proportionately and compliantly to achieve the objectives identified above. The policy will ensure CCTV is routinely monitored, fulfilling a legitimate purpose, visible, well signed, and set up to minimise unnecessary data recording.
- 4.3 The policy will set out the appropriate environment and conditions to use audio recording.

4.4 We will safeguard the data rights of anyone featured in recordings we make.

5 Roles and Responsibilities

5.1 The **Chief Executive Officer** is responsible for ensuring that all the organisation's data processing activities comply with the law and the best practices set out in its policies and procedures.

5.2 The **Data Protection Officer** (DPO) 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.

5.3 The **Head of IT** is responsible for ensuring that all information including video footage, still images, and audio recordings is captured, transmitted, and stored securely.

5.4 **Process owners** are responsible for:

5.4.1 Undertaking DPIAs;

5.4.2 Ensuring the security of CCTV equipment under their responsibility and for complying with this policy and related documentation;

5.4.3 Ensuring the security of the information collected/captured by CCTV equipment they are responsible for;

5.4.4 Ensuring that the CCTV equipment they are responsible for is operating in compliance with this policy and related documents.

5.5 All employees 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 Data Protection Lead any non-compliance that they are aware of or suspect.

5.6 **Senior officers** must ensure recordings are only accessed by those involved in the relevant case and will routinely monitor the use of both CCTV and audio recordings to ensure this.

5.7 **Agencies**, including those who carry out housing management or provide support, operating on Hexagon property using CCTV must demonstrate that they comply with this policy.

6 Use of surveillance equipment

6.1 Any CCTV we use, or used on our property, will be subject to a Data Protection Impact Assessment. This will be used in determining whether to either install or continue using CCTV in a specific area.

- 6.2 We use CCTV for deterring, investigating and preventing crime on our property. We will assess any CCTV to determine whether it provides those functions. We will not install CCTV that does not meet this purpose; existing CCTV may be deactivated or removed if there is no evidence of its effectiveness.
- 6.3 CCTV will be set up to record essential information. We will only record communal areas and will purposely avoid recording sensitive images (for instance, we will not set up cameras that record through windows or doors into a person's home).
- 6.4 All of our CCTV will be clearly visible; we will place signs that are noticeable and legible indicating that CCTV is in operation. We will also be clear about who is operating the CCTV and how they can be contacted.
- 6.5 Any staff accessing CCTV will be trained on operating the system and the relevant responsibilities regarding data protection and human rights.
- 6.6 Where there is a live monitoring screen, this will only be placed in a secure room. Staff with access to the screen will be trained and appropriate measures taken to avoid unauthorised visitors from viewing the screen.
- 6.7 CCTV recordings will only be accessed in response to specific incidents or concerns. Access to the recording will be restricted to officers who are adequately trained and involved in the case. If the incident involves staff, panel members or appropriate senior managers may be authorised view the recorded incident.
- 6.8 CCTV will have time and date stamps to ensure that only the relevant footage is accessed. We will ensure this information is accurate.
- 6.9 Audio recordings must be taken inside the home of a person giving permission. If a neighbour is clearly audible, the recording must be available to them on request.
- 6.10 All recordings (CCTV and audio) will be securely stored and password protected.
- 6.11 Recordings will be deleted after 28 days unless they are required as part of an investigation, legal proceedings or a Subject Access Request.
- 6.12 We will only keep recordings if there is a high likelihood they will need to be played back as part of a case. Alternatives (such as transcription or witness statements) will be always be considered and preferred if appropriate.
- 6.13 We will only share recordings with third parties if they are one of the following:

- 6.13.1 law enforcement (if part of an investigation or to aid the prevention/detection of a crime),
 - 6.13.2 prosecuting agencies or legal representatives (if part of a case),
 - 6.13.3 media (if it is deemed necessary to identify a victim or perpetrator in a criminal incident),
 - 6.13.4 video editing specialist (if we require the video to be edited or anonymised),
 - 6.13.5 another third party (where their needs outweigh those of the individuals whose information is recorded – we will fully consider the risk involved with sharing the information).
- 6.14 If we do share information with a third party, this will be done in a secure format, ensuring access is limited to the intended recipient.

7 Data Subject Access Requests

- 7.1 Data subjects (e.g. those who have been filmed by CCTV or can be heard in an audio recording) may request to view, listen to, or have a copy of recordings in which they feature. This will be treated as a Subject Access Request.
- 7.2 Anyone who makes a request will be provided with general information on Subject Access Requests. They must provide details of the recording they require (such as time, date and location). If the request is excessive or unreasonable they may need to pay a fee.
- 7.3 We will normally provide the recording in which they feature within a calendar month of their request. If the request is complex, we may extend the period.
- 7.4 If the requested recording features identifiable persons other than the data subject making the request, then we will take steps to ensure this data is not inappropriately shared.
- 7.5 We will always do our best to comply fully with Subject Access Requests even if there are other persons featured; we will take reasonable steps such as anonymising footage or removing part of it. However if we believe complying with the request would represent a data breach then we will not be able to fulfil it and this will be explained to the person making the request.
- 7.6 If we require an external service to edit the footage (for instance anonymising for the purposes of a Subject Access Request), a written contract will be drawn up to ensure the security of the data.

8 Monitoring

- 8.1 We will periodically review our CCTV sites and our audio recording procedure to ensure they are justified and appropriate. This will be done through impact assessments and through consultation with our Data Protection Officer.
- 8.2 We will regularly audit our data processing in regard to CCTV and audio recording.
- 8.3 Complaints about CCTV and audio recording will be dealt with through our Complaints policy and procedure.
- 8.4 Hexagon will monitor implementation of this policy as appropriate, and provide relevant training to staff as required.
- 8.5 We will formally review this policy every three years, or sooner if appropriate due to changes in law, regulation or practice.

9 Legal framework

- 9.1 This policy is designed to comply with the following guidance and legislation:
 - Data Protection Act 2018
 - Human Rights Act (1998)
 - Protection of Freedoms Act (2012)
 - UK Government: Surveillance Camera Code of Practice (2013)
 - Information Commissioner's Office: CCTV Code of Practice (2017)
 - United Kingdom General Data Protection Regulation (UK GDPR)

Appendix 1: Equality Impact Assessment

Part one: Initial Screening

Name of policy, service or function	CCTV and audio recording policy
Persons completing initial screening	Policy Officer

Screening

Protected Characteristic	Is impact positive, negative, or none			Reason
	Positive	Negative	No Impact	
Age	X			This policy complies with UK GDPR, Data Protection Act 2018 and the Equality Act 2010 to ensure data relating to protected characteristics is not recorded, shared, or retained unlawfully.
Disability	X			“”
Sex	X			“”
Gender reassignment	X			“”
Race	X			“”
Religion or belief	X			“”
Sexual orientation	X			“”

What are the arrangements for monitoring the policy and its impact on customers?
Regular audits and periodic reviews

As no negative impact has been identified for any group in this screening, we will not proceed to Part 2 of the Equality Impact Assessment.