

CCTV POLICY

1. INTRODUCTION AND BACKGROUND

- 1.1 This policy sets out how ISHA manages its Closed-Circuit Television (CCTV) systems and how we meet data protection requirements.
- 1.2 CCTV is fitted in communal areas to provide security for ISHA residents and to identify perpetrators of anti-social behaviour. CCTV protects our buildings and assets from damage, vandalism, and crime. It supports the police and other agencies in the prevention and detection of crime.
- 1.3 ISHA is the Data Controller of its CCTV systems; in that we make decisions on how the system is used and the information managed. ISHA is also the Data Processor; in that we operate our systems and manage the information collected through our CCTV systems.
- 1.4 The UK General Data Protection Regulation (UK GDPR) sets out a legal binding framework that ISHA and its contractors must comply with. ISHA, its contractors, and individual employees may be held accountable for failure to comply with the law and may be subject to regulatory action including fines and other punishments.

2. SCOPE AND PURPOSE OF THE POLICY

- 2.1 This policy applies where CCTV is installed by ISHA for use in communal areas of our residential sites, the ISHA office locations, and our commercial premises.
- 2.2 As a Registered Provider, ISHA is not subject to the Regulation of Investigatory Powers Act (2000). However, to ensure best practice, we take account of the Information Commissioner's Office (ICO) guidelines.

This policy aims to ensure that:

- Our use of CCTV complies with the relevant legislation and follows best practice.
- Any surveillance cameras are not abused.
- Any system is correctly and efficiently operated.
- In the operation of CCTV at our sites and offices, it is possible that the image of data subjects will be recorded. Therefore, processing is included in our Privacy Notice; on the Housing Data Asset Register and a Data Protection Impact Assessment (DPIA) has been carried out.

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

- To ensure that overt and covert CCTV has a DPIA in place and that all overt CCTV has adequate signage.
- That individuals or 'Data subjects' can access their images on request.
- That information can be used in operational and criminal matters when disclosed to the police or other agencies on their request.

2.4 The use of CCTV equipment will generally be overt, but it may be necessary in some circumstances to use concealed equipment. ISHA recognises that in some cases involving anti-social behaviour, residents can be reluctant to be witnesses in civil or criminal proceedings. The fitting and use of covert cameras can be used as supplementary evidence in both civil and criminal proceedings, and to prove or to disprove allegations.

Overt CCTV

Generally defined as permanent or temporary cameras that are obvious and would be reasonably expected such as security cameras on the exterior of buildings.

Covert CCTV

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, dash cams, 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.
- Data on covert cameras will be accessed by the provider of the equipment.

Excluded Cameras

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. STATUTORY AND REGULATORY FRAMEWORK

- Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation
- Human Rights Act 1998
- Protection of Freedom Act 2012
- Regulator of Social Housing - Regulatory Standards (Neighbourhood & Community Standard)
- Information Commissioner's Office – CCTV Code of Practice
- Home Office - Surveillance Camera Code of Practice

Note: as a Housing Association we are not subject to Regulation of Investigatory Powers Act 2000

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

4. ROLES & RESPONSIBILITIES

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.

The Data Protection Group 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. The Neighbourhoods Team is responsible for monitoring all CCTV installations from their inception through their installation, operation and management and eventual decommissioning on ISHA's estates and the Facilities team is responsible for CCTV in ISHA's office.

The Neighbourhoods and Facilities Teams are also responsible for ensuring that all information including video footage, still images, and audio recordings is captured, transmitted, and stored securely.

Information asset owners are the Neighbourhood Officers and Neighbourhood Manager for overt CCTV on our estates and The Facilities Officer for the CCTV in our offices. They are responsible for:

- Undertaking DPIAs as required by the Data Protection Policy;
- Ensuring the security of CCTV equipment under their responsibility and for complying with this policy and related documentation;
- 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.

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 Group any non-compliance that they are aware of or suspect.

5. DETAILS

5.1 The use of CCTV by ISHA is registered with the ICO (reference no Z8174976). Payment is made to the ICO annually as per the requirements of 'The Data Protection (Charges and Information) Regulations 2018 in the DPA.

5.2 CCTV cameras are to be fitted in communal areas only. CCTV cameras may be placed in areas such as stairways, lifts, entrances communal areas, reception areas and car parks.

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

5.3 CCTV signs are required on all residential and commercial premises to advise ISHA residents and the general public that a camera is present (Appendix 2, CCTV signage).

5.4 Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. No CCTV will be placed in areas where there is an expectation of privacy i.e. bathrooms.

5.5 The Neighbourhood Officer (or Facilities Officer in the case of office CCTV) will arrange standard signage and ensure it is displayed appropriately. If staff identify a CCTV sign which is being displayed inappropriately on our property (i.e. where there is no longer any such equipment installed by or it is not working), then staff should inform the relevant officer.

5.6 If audio recordings are needed in addition to CCTV, the reason why audio is needed should be documented and saved in a safe and retrievable location. ISHA CCTV does not normally record audio.

5.7 Before fitting a new CCTV system or amending a current CCTV system, a Data Protection Impact Assessment (DPIA, Appendix 1) should be completed by the staff member proposing the installation of the CCTV. This will usually be the Neighbourhood Officer. The DPIA will detail why CCTV is needed and how the impact on people's privacy is minimised.

5.8 On installation of CCTV, the Neighbourhood Officer will check the camera angle, to ensure the camera only captures what is needed and nothing more. Footage should be checked to ensure it is clear and detailed.

5.9 CCTV Footage will be kept secure. Equipment will be kept in locked containers and a security code will be needed to access footage.

5.10 CCTV and covert CCTV footage will not be kept for longer than needed. CCTV and covert footage is kept for a period of 38 days. If a request is not made to view the footage it will not be viewed and will be overwritten.

5.11 Requests to view CCTV footage can be made in writing to ISHA stating: who is making the request, the location, date and time of the footage, why the footage is needed. Consideration will then be given to the request to view the data.

5.12 If after consideration it is agreed by either the ISHA Neighbourhoods Manager and/or ISHA Housing Manager that the request is valid, the footage should be released. The Neighbourhood Officer will access the footage stored on site and download the footage for the requested date and time on a USB drive. The USB drive will then be stored in a secure location in the office and disposed of when the footage has been viewed and the request fulfilled.

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

5.13 Where the release of data is disputed between persons making the request and ISHA, ISHA will comply with the request if so ordered by a court order.

5.14 A log will be maintained of all requests made to view CCTV footage. The log will include details such as: the party making the request, the address of the footage/ which camera and where, what date the request was made, the date and time of the footage requested, when the footage was downloaded, who the footage was disclosed to and when it was erased.

5.15 If CCTV footage is stolen or is disclosed to unauthorised parties, the Information Commissioners Office will need to be contacted to report a data breach.

5.16 Where covert cameras have been authorised for use, signage will not normally be erected.

5.17 For covert CCTV, a DPIA will be completed by the instructing ISHA employee, usually the Tenancy Officer. The DPIA needs authorisation from the Housing Manager or the Neighbourhoods Manager. It then needs a final authorisation from the Head of Housing or Director of Housing.

5.18 Covert CCTV footage will be retrieved by the ISHA contractors on the instruction of the ISHA staff member. ISHA may change the contractors that supply and fit CCTV and covert CCTV and retrieve CCTV footage. Storage and erasure of data will be subject to the same process as non-covert CCTV.

5.19 Decommissioning

When CCTV systems are no longer needed, they shall be subject to a decommissioning procedure that includes:

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

6. DISCLOSURE OF IMAGES TO INDIVIDUALS

6.1 CCTV images are personal data and are covered by the UK GDPR. An individual has the right to make a request to view images of themselves, in accordance with the Information Commissioner's Office 'CCTV Code of Practice'.

6.2 Subject Access Requests can also include CCTV digital images which show a recognisable person.

6.3 We will provide images in line with our Subject Access Request process. A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Group at dataprotection@isha.co.uk, who will arrange for a copy of the data to be made and given to the applicant within thirty days of receiving the

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

request. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

7. DISCLOSURE OF IMAGES TO THIRD PARTIES

In limited circumstances, ISHA will share CCTV footage to agencies or individuals on receipt of a Subject Access Request or a Third-Party Disclosure Request in line with our Data Protection Policy.

Sharing of information may occur with the following parties:

Subject Access requests made on behalf of an individual – concerning persons, personal data.

Suppliers and service providers: who manage and operate the CCTV system as our data processor.

Joint data controllers: who may jointly operate and maintain the CCTV system with ISHA, ie. Managing agents

The police and other law enforcement agencies: to carry out policing, assist investigations, trace missing people and investigate criminal activity.

The legal representatives of people who have been injured, attacked or had property damaged or stolen, their insurance providers and the Emergency services: to assist them with any criminal or civil investigations or legal proceedings.

The legal representatives of people who have been involved in road traffic accidents and their insurance providers: to assist with insurance claims legal claims and investigations.

Any relevant regulators: where we are required to do so by law or to assist with their investigations or initiatives, and this includes but is not limited to the Information Commissioner's Office.

We do not disclose personal information to anyone else except as set out above unless we have consent or we are legally obliged to do so. We do not sell personal data.

8. MONITORING AND REVIEW

8.1 All CCTV systems are recorded and kept updated – Appendix 4. All systems are checked quarterly by the Neighbourhood Officer.

8.2 DPIAs are recorded in the DPIA register maintained by the Data Protection Group stored securely in the Neighbourhoods and Data Protection folders.

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

8.3 All requests for CCTV images will be recorded in the register maintained by the Data Protection Group.

8.4 Only staff members listed as having access to CCTV images in the Housing and Facilities Data Registers will have access to images.

8.5 This policy will be reviewed every 2 years or earlier if changes to legislation are enacted.

9. COMPLAINTS PROCEDURE

Complaints concerning use of its CCTV system, or the disclosure of CCTV images will be handled through the ISHA Complaints Policy.

10. TRAINING

Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data. Any training will be at least once a year for staff.

All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake Data Protection training.

11. DATA SUBJECT RIGHTS

As a controller of personal data, all the rights afforded to data subjects under the GDPR will apply to the organisation and its use of CCTV. In relation to this specific activity the European Data Protection Board (EDPB) has provided some added clarification for some of the data subject's rights as follows:

11.1 Access rights

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. The organisation may also ask the data subject to specify reasonable timeframes to help with information searches.

11.2 Right to erasure

The EDPB notes that blurring a picture with no retroactive ability to re-convert the picture into an identifiable image constitutes erasure in accordance with GDPR. ISHA will confirm in writing to the data subject that the image has been deleted.

11.3 Right to object

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

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024

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.

12. EQUALITY AND DIVERSITY

ISHA will demonstrate its commitment to equality and diversity in implementing the CCTV policy. We will ensure that nobody receives less favourable treatment on the grounds of age, disability, gender reassignment, pregnancy & maternity, race, religion or belief, sex or sexual orientation.

13. ASSOCIATED DOCUMENTS

Appendix 1: ISHA DPIA (Data Protection Impact Assessment)

Appendix 2: CCTV and Privacy notice Template

Appendix 3: ISHA Customer Privacy Notice

PROPOSED Appendix 4: List of all ISHA sites with CCTV systems

Reference	Version	Created	Author	Review	LT Approved
CCTV Policy	1	September 2023	Aisling Hodson	February 2027	February 2024