Title:	CCTV Policy
Person responsible:	Governance and Risk Manager
Customer consultation arrangement:	Consultation via survey
EIA required:	Yes
EIA completed (date):	21/02/25
Approved by:	Senior Management Team
Business Strategy Objective	Transforming
Approval date:	April 2025
Links to other key policies:	Data Protection & Data Privacy Policy ICT Policy Tenancy Management Policy Anti-Social Behaviour Policy
Review date:	April 2028

Document management

Version	Date amended	Amendments
1	April 2025	Original

1. Purpose and Scope

1.1 This policy outlines South Lakes' Housing's (SLH's) approach to closed circuit television (CCTV) and other video surveillance systems. It sets out how CCTV images are collected, used and stored. It outlines the controls required to ensure compliant operation of systems. It covers:

- Commercial video surveillance systems, monitoring offices and work premises
- Residential video surveillance systems, located on schemes managed by SLH in communal or public areas

It applies to all systems installed by (or on behalf of) SLH. Domestic CCTV systems, smart camera doorbells and video surveillance footage collected by customers do not fall within the scope of the main body of this policy, but these areas are covered within the appendices.

Vehicle reversing aids (where there is no recording of images) and broadcast video cameras (used for collecting footage for promotional purposes/videos/training) are excluded from the scope of this policy.

1.2 In operating CCTV systems, SLH's objective is to balance the privacy rights of individuals with the organisation's responsibility to prevent and detect anti-social behaviour and other criminal activity; as well as to protect the personal safety of customers and colleagues. South Lakes Housing utilises CCTV with the aim to:

- Deter and detect criminal activity
- Prevent and tackle antisocial behaviour
- Promote the personal safety of our customers
- Protect the health, safety and security of colleagues
- Assist in the detection of crime and identification of individuals by providing CCTV footage to relevant authorises to enable them to take law enforcement action

Video surveillance will not be used or approved for any purpose that might conflict with these aims. SLH will carry out an annual data privacy review of CCTV deployment to ensure it is proportionate to these aims and meets the requirements outlined in this policy.

2. Regulatory and Legislative Requirements

2.1 SLH's approach to CCTV and video surveillance will comply with all legal and regulatory requirements, with particular reference to the following:

- Data Protection Act 2018
- UK General Data Protection Regulation (GDPR)
- Equality and Human Rights Act 2010
- Regulatory and Investigatory Powers Act 2000

Under data protection law, video surveillance footage is considered personal data as it may directly identify an individual.

3. Definitions

3.1 Video surveillance systems specifically include, but are not limited to:

- Traditional CCTV
- Automatic number plate recognition
- Body worn video
- Drones
- Vehicle dashcams
- Smart camera doorbells
- Action cameras (inc. mobile phone cameras, web cams, goPro devices)

The terms used in this policy have the meanings attributed to them in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

4. Our Approach

4.1 SLH will use video surveillance only where it is a proportionate and necessary measure to achieve a defined business objective. Surveillance will only be commissioned in accordance with this policy and related work instructions and procedures. The approach outlined below applies to residential and commercial video surveillance systems only. Refer to Appendix A for guidance on SLH's approach to domestic CCTV and Smart Camera Doorbells. Refer to Appendix B for guidance on customer recordings.

4.2 Commissioning

4.2.1 Prior to the introduction of any new CCTV or video surveillance systems:

- A data protection impact assessment (DPIA) will be undertaken to ensure there is critical analysis of the legitimacy and need for the system being proposed, as well as to highlight and mitigate any potential risks to the privacy, rights and freedoms of individuals. The suitability of the location proposed will be considered.
- Where legitimate interest is identified through the DPIA as the 'Lawful Basis' for the use of CCTV or video surveillance, then a Legitimate Interest Impact assessment will be completed.
- Due diligence checks will be carried out to ensure the proposed video surveillance system has:
    - Tamper-proof cameras, cables, transmission equipment and data storage
    - Access controls and the data retention policy outlined in the DPIA is effective
    - Appropriate signage in place (see section 4.4.2)

4.3 Approval, Installation and Recording

4.3.1 Approval for the installation of any video surveillance system must be sought from the Director of Business Improvement (Data Protection Officer) who will consider the case put forward by the relevant manager, alongside input from the Governance and Risk Manager and the Systems and Change Lead. In their absence, the decision for approval must be obtained from another Director.

4.3.2 This approval pathway applies to requests from partner organisations, including local authorities, to install video surveillance systems on land which is the property of SLH.

4.3.3 Installation of CCTV equipment must be carried out by a suitably skilled member of the SLH repairs and maintenance team or an approved contractor.

4.3.4 The Systems and Change Lead is responsible for maintaining a register of all CCTV installations for which SLH is either a data controller or a data processor. They will ensure all relevant information is captured, including but not limited to:

- Location
- System specification

- A defined owner
- Still images of the field of view of each camera for use as a future field of view reference point

4.4 Communication with customers on CCTV Installation

4.4.1 If it is deemed fair, lawful and appropriate to install CCTV on a residential estate SLH will contact residents to confirm:

- The purpose of the CCTV system
- That appropriate authorisation and controls are in place
- Whether it is a temporary or permanent installation
- Who to contact if customers have a concern or enquiry about the CCTV system

Where possible, customers will be consulted prior to installation of the system. SLH will fully consider alternative options before deploying video surveillance technology. Where a Legitimate Interest Assessment has been completed (see section 4.2.1) a copy of this will be made available to customers upon request.

4.5 Privacy Information

4.5.1 Other than in select circumstances where covert CCTV may be used (see section 4.7), SLH will ensure privacy information is displayed prominently to ensure people are made aware of the use of video surveillance whilst they are within its field of view. The Data Protection Officer is responsible for ensuring appropriate privacy information is created and installed.

4.5.2 Signage should provide a clear visual indication that video surveillance is in place and should be positioned in such a way that the data subject can easily recognise the circumstances of the surveillance before entering the monitored area. The signage should at a minimum provide:

- A warning that CCTV is in operation
- The purpose of the CCTV installation
- The name of the data controller (i.e. SLH)
- Contact details for further information

4.5.3 All information under Article 13 of the UK GDPR must be easily available upon request by the data subject and may be displayed on a poster or at a nearby information desk. This will include, but is not limited to:

- Data retention period
- Rights of data subjects

4.6 Operating CCTV Installations

4.6.1 *Data Retention and Storage*

SLH will ensure that by default, CCTV footage is retained for no longer than 31 days. However, this will be reviewed on a case by case basis, new

installations in the community may require a longer retention period for example to assist with case management. Images required for an investigation shall be removed from the CCTV storage system and kept in a specific storage system for CCTV images under investigation. These shall be retained for no longer than 2 years following the end of the investigation. The Data Protection Officer shall maintain a register of CCTV images stored for investigation.

4.6.2 *Security*

The Systems and Change Lead shall ensure that technical measures are in place to ensure all CCTV images are adequately protected from accidental or unlawful destruction, loss, or alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed through the implementation of technical and organisational controls and measures.

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 the organisation, including access controls, user authentication, anti-virus and malware software, penetration testing etc.

4.6.3 *Viewing recorded CCTV Images*

Recorded CCTV images shall only be reviewed where there is a defined business need.

Requests to review recorded CCTV images shall be submitted to the Data Protection Officer. Where the Data Protection Officer determines that the request is valid, they shall arrange for the CCTV images to be available for viewing.

The viewing of recorded CCTV images shall take place in a restricted area (e.g. private office). Other parties should not be allowed to have access when a viewing is taking place.

4.6.4 *Viewing live CCTV Images*

The organisation 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. community surveillance).

The live feed for CCTV images in the Office can be viewed from behind reception. The live feed for video surveillance systems installed in the community will have restricted access, either terminating in a secure area with access limited to specific designated personnel, or a remote feed with access restricted to relevant persons.

4.6.5 *Disclosure of CCTV Images*

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

Any colleague in receipt of such a request shall pass it to the Data Protection Officer. The Data Protection Officer will maintain a register or all requests for CCTV footage disclosure and how they were handled.

The Data Protection Officer will assess each disclosure request on its merits and shall always exercise the highest degree of scrutiny and caution so as to ensure the rights of people who feature in the footage are not compromised.

In assessing each request for disclosure, the Data Protection Officer shall consider:

- The purpose of the request, the aim of the requestor and the proposed use of the requested footage;
- The organisation's lawful grounds for disclosure;
- The rights of individuals which may favour non-disclosure;
- The necessity of the disclosure to further the requestors' purpose.

Requests for disclosure shall always be made in writing or written confirmation obtained to support verbal requests.

Disclosures made as part of a Data Subject Access Request shall ensure that no images of third parties are provided to the data subject making the request. Third parties must be anonymised using appropriate technical measures such as those advised by the European Data Protection Board or other relevant body (for example the scrambling or pixilation 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).

After considering all factors associated with the request, the Data Protection Officer shall decide whether the footage should be disclosed and any terms relating to the disclosure. Where copies of images or recordings are disclosed, they will be sent securely via an encrypted channel.

4.6.6 *Maintenance*

CCTV installations shall be subject to a structured schedule for routine maintenance undertaken by an appropriately qualified contractor.

4.7 Decommissioning

When video surveillance systems are no longer needed, they will be subject to a decommissioning procedure which includes:

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

Decommissioning will be carried out in accordance with SLH's Technology Equipment Disposal Procedure.

4.8 Covert Video Surveillance

4.8.1 Covert video surveillance includes cameras that are deliberately hidden to avoid detection or that may not be obvious (or obviously collecting footage) such as drones, dashcams, GoPros or mobile phones.

4.8.2 The Regulations of Investigatory Powers Act 2000 governs the use of covert surveillance to ensure it is used only, when necessary, reasonable and proportionate. Whilst it does not apply to housing associations, SLH will follow the legislation as closely as reasonably possible. SLH will only use covert video surveillance in extreme circumstances, in conjunction with agencies such as the Police, for the purpose of an ongoing investigation or operation. SLH will ensure a balance between an individual's reasonable expectation of privacy and the necessity to gather evidence covertly. The same rules as at sections 4.1 to 4.3 apply to covert CCTV, except:

- No signage will be displayed
- SLH have no obligation to alert any individuals covert CCTV is in use
- The use of covert CCTV will be time limited (as specified at the point of authorisation)
- SLH will perform frequent compliance reviews of the covert CCTV

4.8.3 Schedule 2, 3 and 4 of the Data Protection Act 2018 contain exemptions to the requirement to provide privacy information. The Data Protection Officer shall ensure there is a written justification for all instances of CCTV implementations where privacy information is not provided.

4.9 Requests and Queries from Customers

4.9.1 As a general rule, standalone requests for SLH to install residential CCTV will be refused unless they is a clear case for why installation is necessary, linked to a reported instance/ instances of anti-social behaviour. In these circumstances installation of CCTV will be considered in line with this policy.

4.9.2 For any queries or concerns regarding CCTV, customers should contact their neighbourhood partner in the first instance.

5. Responsibilities

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

5.2 The Data Protection Officer is responsible for defining work practices that are compliant with the law and best practices by 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 management and eventual decommissioning.

5.3 The Systems and Change Lead is responsible for ensuring that all information including video footage, still images, and audio recordings is captured,

transmitted, and stored securely. They are also responsible for maintaining a register of CCTV systems, with each system allocated a defined owner.

5.4 The defined owner for each system is responsible for:

- Undertaking DPIAs and Legitimate Interest Assessments as required by the Data Protection Officer
- Ensuring the system is operating in compliance with this policy and related documentation
- Working with the Data Protection Officer and Systems and Change Lead to swiftly address any concerns or areas of potential non-compliance, should they arise

5.5 All colleagues are responsible for complying with this policy and related procedures and instructions. All colleagues are responsible for reporting to the Data Protection Officer any non-compliance that they are aware of or suspect.

6. Monitoring & Review

6.1 A series of checks will be undertaken to verify the compliance of video surveillance systems with this policy:

- Quarterly still to live image check
- Quarterly data retention check
- Quarterly privacy information check
- Periodic re-evaluation of the need (in line with DPIA findings)
- Annual check of maintenance records

6.2 This policy will be reviewed every three years, or where there have been significant changes to regulation, legislation, operations or best practice to warrant a further policy review.

Appendix A: Domestic Video Surveillance Systems and Smart Camera Doorbells

1.1 Customers must obtain South Lakes Housing's (SLH's) permission as their landlord, before installing domestic video surveillance including doorbell cameras if it involves adaptation to their property. Adaption is defined in accordance with the conditions of the customer's tenancy agreement or lease.

1.2 Each request will be considered on a case by case basis and no equipment should be installed unless such permission is granted. The Neighbourhood Manager will be responsible for considering requests and making the decision as to whether to grant approval. In their absence, the decision will sit

with the Head of Neighbourhoods. Customers will be notified of the decision outcome in writing.

1.3 SLH will not unreasonably withhold permission for the installation of domestic CCTV systems. Where possible customers should position their cameras to only capture their own property. Where customers install devices which record public or communal spaces (i.e. anywhere outside the boundary of the customer's property, including corridors within blocks of flats), the customer takes on responsibility as a Data Controller in operating the system. As such, they must:

- Assign and document the lawful basis for the processing of personal data under Article 6 of the UK GDPR. Ensure processing is in accordance with the identified lawful basis.
- Provide appropriate privacy information, including signage to tell people they are being recorded
- Comply where possible with requests for disclosure of recorded footage from data subjects or with requests by data subjects for them to stop being recorded or for footage containing them to be deleted
- Regularly or automatically delete footage

1.4 Customers should be aware that failure to meet these requirements could result in individuals affected by the processing bringing civil actions against them, resulting in a fine and a court order to stop using the device. If SLH become aware of a customer or third party using domestic video surveillance systems in an inappropriate way that meets the threshold of harm outlined in our Anti-Social Behaviour Policy then SLH will take appropriate action in line with this policy.

1.5 The following conditions will be communicated to customers if permission is granted for the installation of a domestic video surveillance system:

- Customers must ensure all installation works are carried out by a competent person, having the knowledge and ability to work within current building regulations
- Installation of the device must not cause structural damage to the property or compromise the fire safety integrity of the building. Devices must not be installed by screwing or drilling into the customer's front door, door frame or fire-retardant cladding
- When vacating the property customers must ensure the system is removed and the property reinstated to its original condition prior to the termination of their tenancy

1.6 Appropriate tenancy enforcement action will be taken should any of the conditions above be breached. This may include recharges for reasonable costs.

1.7 Where permission is granted for installation of devices inside customers' homes (which do not film public spaces), the customer does not take on the responsibilities of a data controller so is not required to enact the measures listed in section 1.3. However, customers are advised that they should tell

SLH staff or contractors who enter their homes that they are being filmed. Colleagues are authorised to stop doing any work that they reasonably suspect is being recorded. Customers should be aware of the implications of this and how it could impact their receipt of essential services.

Appendix B: Ad Hoc Video and/or Audio Recording by Customers

1.1 When working with customers who have reported antisocial behaviour, South Lakes Housing may ask the customer to send through evidence to be able to investigate the report and take appropriate action. This may include photos, videos or audio recordings. We may ask customers to share recordings with SLH, either directly or via the Noise App. Colleagues must be mindful that the data they receive via these channels is classed as personal data and must be processed in accordance with SLH's Data Protection Policy.

1.2 Customers should never be asked to film, photograph or collect audio of people if doing so intrudes into their home as this would be an invasion of privacy. For example, customers should never be asked to take footage through someone else's window or aimed at someone's front door.

1.3 Taking photographs or filming people in a public place wouldn't usually be considered an invasion of privacy and it may be appropriate for customers to record or photograph people if damage is being caused to their property or if they're causing nuisance to the customer in a public place.

1.4 Customers and colleagues should be mindful of the following:

- It is illegal to take, make, distribute, show, display, publish or possess indecent photographs of anyone aged under 18, as defined in law
- Photograph or video evidence should only be used for the purpose of assisting authorities (including SLH) in preventing or detecting Anti-social behaviour. It should not be used for publishing or wider use, especially if it identifies people. Once customers have shared the evidence with relevant agencies, they should delete it from their phone
- A person cannot claim they're being harassed because they were photographed or filmed when they did not want to be. But if it causes alarm and distress, and if a pattern of behaviour is established it could then be viewed as harassment. For example, if you film someone on a number of occasions without any basis on which to do so.

Appendix C: CCTV Register

Camera ID	Location	Device Type	Model	Serial Number	Installation Date	Installer	Field of View Description	Retention Period	Access Control
1	Reception	Motion Detected	Reolink NVR 8CH		10/4/24	SLH IT	Reception Area	No longer than 31 days	Restricted to IT for recording, open to all staff to view on TV screen
2	Interview Room 1	Motion Detected	Reolink NVR 8CH		10/4/24	SLH IT	Interview Room 1	No longer than 31 days	Restricted to IT for recording, open to all staff to view on TV screen
3	Interview Room 2	Motion Detected	Reolink NVR 8CH		10/4/24	SLH IT	Interview Room 2	No longer than 31 days	Restricted to IT for recording, open to all staff to view on TV screen