CCTV Policy

1.0 Introduction

1.1. This Policy outlines our approach to the use of residential closed-circuit television (CCTV) and other video surveillance systems (see 2.2). It sets out how we'll collect, use, and store CCTV images and information. It covers:

- Residents with an occupancy agreement with us, including Independent Living Schemes and where Southern Housing is acting as a managing agent
- Third-party suppliers who install, maintain, operate, or remove CCTV on our behalf
- Existing and future installations of overt (visible) and covert (hidden) CCTV, both fixed and mobile
- Existing and future domestic CCTV systems and smart camera doorbells installed by our residents themselves.

1.2. This Policy does not cover:

- The operation of commercial CCTV systems monitoring offices and work premises owned, managed, or leased by Southern Housing (this is covered in the Facilities Operating Procedure)
- The use of 'dummy' or non-operational CCTV systems, as no images or information will be processed
- CCTV systems installed or proposed by third parties (e.g. commercial premises owners or operators, owners or agents of residential blocks or estates and/or similar) in areas (such as their buildings and/or on their land) they control and/or over which we have no responsibility or control even if there is an obligation to contribute to such systems if they arise.

1.3 Subject to section 1.1, whilst CCTV systems owned by the Facilities Team and used to monitor work premises are out of scope for this Policy, we recognise employees and contractors may, as part of their standard work routines, be captured on Southern Housing residential CCTV systems and private resident-owned camera doorbells or mobile devices. Residents should be mindful:

- An employee or contractor can decline to be recorded
- Any filming of an employee or contractor should not interfere with or prevent work being carried out
- We may take tenancy action where filming causes interference or obstruction to work being carried out

- We may take legal action if video footage of our employees or contractors is disclosed to unauthorised third parties.

Colleagues with concerns or queries regarding use of cameras should contact the Data Protection Team for support.

1.4 Where we use 'you' and 'your' in this Policy, we mean our residents. The terms 'we', 'our' and 'us' mean Southern Housing.

1.5 Where we use the term 'CCTV' and 'CCTV system', we refer to overt (visible) CCTV. For specific information on our use of covert (hidden) CCTV, please refer to section 6.

1.6 Our objective is to balance the privacy rights of residents and individuals with our responsibilities to:

- Prevent and detect anti-social behaviour and other criminal activity
- Protect the personal safety of our residents and reduce the fear of crime.

Therefore, we utilise CCTV with the aim to:

- Deter and detect criminal activity
- Prevent and tackle anti-social behaviour
- Promote the personal safety of our residents and reduce the fear of crime
- Protect the health, safety, and security of our staff
- Protect the asset value of our buildings and developments
- Assist in the detection of crime and identification of individuals by providing CCTV footage to relevant authorities to enable them to take law enforcement action.

1.7 We'll not use CCTV for any purpose that might conflict with these aims. We conduct a data privacy review of our CCTV deployment as a minimum once a year, or otherwise appropriate to the specific timeframes, to ensure it's still necessary and proportionate to these aims.

1.8 For more information on your privacy rights associated with our processing of CCTV images and information, please refer to Southern Housing's Privacy Notice and Data Protection Policy.

2.0 What is meant by a camera or video surveillance system

2.1 A surveillance camera system means a closed-circuit television or any other system for recording or viewing visual images and information. It can be any system for, but not limited to:

- Storing
- Receiving
- Live-streaming
- Transcoding
- Processing
- Checking images and audio information.

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

- Traditional CCTV
- Automatic Number Plate Recognition (ANPR)
- Body Worn Video (BWV)
- Drones (UAVs)
- Vehicle dashcams
- Smart camera doorbells
- Action cameras, such as GoPro or other portable devices.

2.3 We do not normally use video surveillance to directly record audio information and all our surveillance systems have audio recording switched off by default. We'll only record audio via video surveillance when tackling anti-social behaviour and other criminal activity. In addition, we'll use audio recording equipment where we have:

- Two-way audio feeds from 'help points' covered by CCTV
- Where we trigger recording due a specific threat, for example on a lone-worker alert system, such as a PeopleSafe personal safeguarding device.

2.4 Where audio recording is initiated, we'll clearly communicate it's in use (except where covert (hidden) recording is being used, see section 6.

2.5 We'll ensure our use of CCTV or other video surveillance systems is balanced and proportionate to the impact of anti-social behaviour and other criminal activity on individuals and communities. One of the ways we do this is to ensure our use of CCTV complies with UK rules and regulations, official guidance, and data protection law. This is because video surveillance footage is considered personal data under data protection law, as it may directly identify an individual. Relevant regulation and legislation specifically include, but are not limited to:

- UK General Data Protection Regulation (UKGDPR)
- Data Protection Act 2018 (DPA 2018)
- Surveillance Camera Code of Practice (Feb 2022) (PoFA 2012)
- Regulation of Investigatory Powers Act 2000 (RIPA 2000)
- Information Commissioner's Office guidance.

3.0 Ensuring compliance with UK regulation and data protection law

3.1 One way we ensure compliance is to fully consider alternative options before installing any video surveillance system. We'll assess other options to address the issues, such as improving lighting, upgrading fencing, or increasing security patrols. We'll only propose the installation of CCTV where the alternatives do not sufficiently address the relevant issues.

3.2 In addition, for every CCTV installation, we'll:

- Conduct a Data Privacy Impact Assessment (DPIA) to assess the data protection implications and identify the risks associated with processing your personal data in this way

- Ensure the installation is not in an inappropriate location where you would reasonably expect privacy, such as in toilets or changing rooms
- Perform due diligence checks to ensure the CCTV system has 'privacy-friendly' functionality and these are all set appropriately
- Comply with the Surveillance Camera Code of Practice 2022 and related guidance on the Biometrics and Surveillance Camera Commissioner's website
- Conduct an annual visual check of the CCTV system to ensure operational effectiveness, for example that the field of view is not physically blocked
- Conduct an annual technical check of the CCTV system to ensure it is working correctly, for example that the system is time and date stamped accurately
- Ensure the system can capture images of sufficient quality to enable identification of individuals for law enforcement purposes
- Display clearly visible CCTV signage confirming we are the controller of the system and we are responsible for how it is used under UK regulation and data protection law
- Implement a 'data protection by design and default' approach, putting in appropriate technical controls to support data protection principles prior to installation.

4.0 Consultation with residents on CCTV installation

4.1 If we consider it fair, lawful, and appropriate, in all the circumstances to install CCTV on a residential estate or in a communal area, we'll contact residents to confirm:

- The purpose of the CCTV system
- We have the appropriate authorisation to install CCTV
- We have the appropriate controls in place to keep the CCTV data secure
- Whether it's a temporary or permanent installation
- Whether there is a cost recoverable from a service charge for the CCTV system - in such cases, we'll formally consult residents on the costs
- We have done all the things we said we'll do in 3.2
- Who to contact if a camera is damaged or if a camera's field of vision has become physically blocked
- Who to contact if you have an enquiry about the CCTV system.

4.2 Under data protection law, you have the right to access and receive a copy of your personal data; this may include images and information captured by any overt CCTV system we have in place if it can identify you as an individual. This is called the right of access and is commonly known as making a Subject Access Request or SAR.

The easiest way to make a SAR is by contacting us at data.protection@southernhousing.org.uk. We are not able to release images or information of other people to you and so you may receive only part of the information you asked for.

4.3 We'll fully consider alternative options before deploying other video surveillance technology, such as the systems listed in 2.2. We'll assess other options, such as extra or improved traditional CCTV systems or improved staff training and we'll only propose using other video surveillance systems where the alternatives do not sufficiently address the relevant issues. If we consider it fair, lawful, and

appropriate, in all the circumstances to use another form of video surveillance, wherever possible, we'll consult with you specifically on that system.

4.4 How we'll use other video surveillance systems is documented in Appendix 1.

5.0 Ensuring effective control of our video surveillance systems and footage

5.1 Only staff authorised and trained to operate CCTV equipment can review, download, and share footage data at a local level.

5.2 We'll use appropriate technical and organisational measures to ensure the security of the footage data we hold. We'll ensure all electronic files containing CCTV footage are password protected and CCTV control rooms are securely locked.

5.3 We hold and maintain a centralised database of all our CCTV installations and staff authorised to operate our CCTV equipment. We view this list as a 'living document' and constantly review and update this information to ensure it is accurate and that our use of CCTV in each location remains necessary and appropriate.

5.4 We'll remove a CCTV installation at the earliest opportunity where it is no longer necessary or appropriate for its original purpose. A request for removal of a CCTV installation can come from an employee or a resident. We'll consult with local residents before removing fixed cameras in residential areas.

5.5 We take a privacy-friendly approach to any CCTV installation. We'll only install a system where we can control video and audio recording independently to ensure these data streams are separate and processed appropriately.

5.6 We'll deal with any data breach involving CCTV video footage in line with our internal data breach procedure.

5.7 We'll only share CCTV video footage in a secure manner and only with authorised organisations. We'll share video footage for the purposes of administration of a legal claim, for example with an insurance company, a health and safety investigation, or to comply with a civil court order. We'll also provide the police with video footage in the course of a criminal investigation.

5.8 We enforce a strict retention period for CCTV and video footage and information, which is consistent with our purpose and objectives of processing that data. We'll only keep the data for the minimum period necessary for the purpose(s) we legitimately use it and for a maximum of 31 days. After which we'll permanently erase all data unless the information relates to an ongoing investigation or legal proceedings. In which case, we'll permanently erase the data within three months of closing the investigation or any legal proceedings concluding.

5.9 We'll keep a record on our internal data privacy management systems when we:

- Download, review, and redact CCTV and video surveillance footage
- Disclose CCTV and video surveillance footage legally to a third party
- Copy or move the data to another location
- Process a Subject Access Request
- Install a new CCTV or video surveillance system

- Remove a CCTV or video surveillance system
- Receive a query or complaint from a resident regarding a CCTV or video surveillance system
- Comply with a request from a law enforcement agency requiring disclosure of CCTV and video surveillance footage.

6.0 When we use covert (hidden) CCTV

6.1 We'll only use covert (hidden) CCTV in circumstances where it is strictly necessary and proportionate, and when alternative methods of gathering evidence of criminal activity, such as tenancy fraud or anti-social behaviour, have not been successful. In most, but not all cases, this will be in consultation with or in response to a request from the police or other law enforcement agency.

6.2 Whilst Southern Housing does not generally operate under the requirements of RIPA 2000 as it relates to covert surveillance, we have broadly adopted the obligations within the Act as best practice guidance when using covert CCTV. This means using covert surveillance strictly for the purpose of an ongoing investigation or operation, and ensuring a balance between an individual's reasonable expectation of privacy and the necessity to gather evidence covertly.

6.3 The same rules as at sections 3.2 and 4.1 apply to covert CCTV, except:

- No signs will be displayed
- There's no obligation to alert any individuals covert CCTV is in use
- The use of covert CCTV will be time limited as part of the authorisation in 6.4
- We'll perform a more frequent compliance review of the covert CCTV, consistent with the limited time frame.

6.4 A Leadership Team member will authorise the use of covert CCTV when it's to be used in residential areas. We'll ensure effective compliance monitoring of the covert surveillance throughout its duration.

6.5 We'll only record sound via covert CCTV where it is strictly necessary for the purpose of evidence gathering or where it is formally requested by the police in the course of an investigation.

7.0 Unauthorised CCTV installation by a third party

7.1 If a third party installs CCTV or other video surveillance in an area we're responsible for without our knowledge or authorisation, within five working days of becoming aware, we'll:

- Begin investigating who installed the CCTV and seek legal advice on our options for removing it
- Initiate arrangements for clear signage to be placed in the affected area, advising that CCTV is in operation
- Contact all affected residents and advise we're investigating who installed the CCTV with a view to legally removing it
- Provide a timeframe for removal of the CCTV where possible

- Continue to update affected residents at least once every three weeks until the situation is resolved.

8.0 Residents installing and operating domestic CCTV and smart camera doorbells

8.1 You are legally entitled to install CCTV or a smart camera doorbell for your domestic use only and you do not need to contact us where you intend to do so, **provided**:

- Your tenancy or rental agreement states you can make any adaptions to your property without our express permission
- The installation of a smart camera doorbell can be done without causing any damage to the structure of the building or compromising the fire-safety integrity of the building
- Your lease agreement with the leaseholder states you can make any adaptions to your property (where Southern Housing is acting as a managing agent)
- You comply with the requirements listed in 8.2 and 8.3.

If you are in any doubt about the requirements of installing a camera doorbell, please contact data.protection@southernhousing.org.uk. Any breach of these stipulations may result in the removal of the doorbell camera and you being charged for any repair work required.

8.2 If you operate a domestic CCTV system or smart camera doorbell, you must:

- Ensure the camera is installed next to the door of your property, **but not on the door frame itself,** and it must be within the legal boundary of the property
- Take responsibility to ensure installation of the camera does not cause structural damage to the property or compromise the fire-safety integrity of the building
- Wherever possible, ensure the camera only captures images and information of individuals visiting your property within the area of the front door
- Wherever possible, point cameras away from neighbours' properties, especially their doors and windows, gardens, communal areas, shared hallways, or public areas. Where this is not possible, carefully consider how intrusive the camera is for other residents and comply with all stipulations in 8.1 - 8.3 at all times.
- Set a privacy blur filter on the recording device as per the set-up instructions (if available) to limit the accidental capture of individuals where possible
- Remove any CCTV equipment or doorbell camera if you are vacating the property and ensure the device is deactivated and you no longer have access to the video footage
- Comply, wherever possible, with a request for video footage on your device from a member of the public, a neighbour, or agency. Southern Housing are unable to make the access request on behalf of that person or agency or force the camera owner to provide any video footage.

8.3 If you operate a domestic CCTV system or doorbell camera, under data protection law you are the controller of the data you collect. This means you own the video footage and are legally responsible for what happens to it. In order to comply with data protection regulations, you must:

- Not share any domestic camera footage on social media
- Only share camera footage with an authorised organisation such as Southern Housing or law enforcement agencies, unless it is in response to a formal request from an individual for their personal data only
- Put up signage that you are operating a domestic camera system
- Regularly or automatically delete footage
- Stop recording an individual if they object to being recorded, but only if it is possible to do so. For example, if you can point the camera in a different direction, but still use it for the same purpose, such as safeguarding your property.

8.4 Failure to meet these requirements may be a breach of your occupancy agreement. We may ask you to remove the domestic camera system, and if you do not, this may result in legal action being taken to remove it and you being charged for any repair work required.

8.5 Where Southern Housing is acting as a managing agent and the leaseholder has advised residents they are prohibited from making alterations to the property, including installing camera doorbells, Southern Housing is unable to intercede on behalf of the residents and the leaseholder is entitled to enforce the terms of the lease.

8.6 If we are notified of a resident or a third-party installing a doorbell camera in an inappropriate location or using a doorbell camera or other device in a way that goes beyond our harm threshold of harassment or intimidation as defined in our Anti-social Behaviour Policy, we'll:

- Initiate an investigation at the earliest opportunity
- Take whatever action is appropriate on a case-by-case basis.

8.7 If you share domestic CCTV or doorbell camera footage with us to report an incident, we'll only initiate an investigation where the footage clearly shows anti-social behaviour or other criminal activity that goes beyond our harm threshold. We shall take whatever action is appropriate on a case-by-case basis.

8.8 For more information and guidance on domestic CCTV and doorbell camera use, please visit the ICO's website.

9.0 Concerns or queries about our CCTV and video surveillance systems

9.1 For any queries or concerns about CCTV or video surveillance, please contact your Housing Officer, Scheme Manager, or equivalent in the first instance.

9.2 If you remain dissatisfied with our response you can follow Southern Housing's Complaints Policy or contact the Information Commissioners Office for advice.

9.3 We will respond to any formal request for statistical information regarding our CCTV on a case-by-case basis.

9.4 A paper copy of this Policy is available upon request by contacting Southern Housing.

10.0 What we've done to ensure this Policy is fair

10.1 We've carried out an Equality Impact Assessment to consider the positive and negative impacts this Policy may have on people with protected characteristics under the Equality Act 2010.

10.2 We recognise some residents may need adjustments due to a language barrier, disability, cultural need, or vulnerability. In these circumstances, in line with our Reasonable Adjustments & Vulnerable Needs Policy, we'll work with residents to ensure we consider their specific needs, on a case-by-case basis, provided it doesn't compromise health and safety to individuals or homes. This includes working in partnership with other agencies to ensure we manage and mitigate any known risks of safety and wellbeing.

10.3 We aspire to embed diversity and inclusion within the culture of our business activities.

11.0 Review

11.1 We will review this Policy to address legislative, regulatory, best practice or operational issues.

12.0 Appendices

Appendix 1 – types of video surveillance

Policy controls
Version 1.2 – effective 7 October 2025

Appendix 1 – types of video surveillance

Automatic Number Plate Recognition (ANPR) systems can analyse vehicle number plates and cross-reference those details with live databases across the UK. We may use ANPR, for example to identify you as holding a car park permit and allow your vehicle access to a restricted car park.

Body Worn Video (BWV) systems are often attached to clothing or a uniform and can capture both visual and audio information in close proximity to the individual. We may use BWV, for example where an individual is being aggressive towards our staff.

Drones or Unmanned Aerial Vehicles (UAVs) are remotely piloted aerial cameras that can capture images and geographical information from a high vantage point. We may use or authorise third-party use of UAVs, for example to inspect damage to a roof of one of our properties.

Vehicle dashcams are small inward or outward facing cameras mounted in a vehicle with the capability of recording footage of a journey and any incidents that might occur. We may use a vehicle dashcam, for example to record footage of a road traffic incident.

Action cameras could include mobile phone cameras, web cams, GoPro devices or other action cameras. They have similar capabilities to BWV and can be used in similar ways. We may use an action camera, for example to record footage of an incident where traditional CCTV is not available.

If we think it's necessary, proportionate, and lawful to use one of these options, we'll:

	ANPR	Body Worn Video	Drones or UAVs	Dashcams	Action cameras
Explain the reasons and purpose of using this system	✓	✓	✓	✓	✓
Conduct a Data Privacy Impact Assessment (DPIA) that fully addresses our use of the system	✓	✓	✓	✓	✓
NOT retain footage, images, or information any longer than is strictly necessary for the intended purpose	✓	✓	✓	✓	✓
Put clear signage in place, including detail of who to contact if you have a query	✓		✓	✓	
Give sufficient privacy information (e.g. verbal announcement or lights/indicators on the device)		✓	✓	✓	✓
Train our staff using the system to inform individuals recording may take place if it's not obvious in the circumstances		✓		✓	✓
Use the system in a way that minimises the risk of accidental filming of residents	✓	✓	✓	✓	✓
Ensure locations are justifiable and placed to minimise the risk of accidentally capturing any vehicles not of interest	✓				