

Reliance Social Housing CIC

CCTV Policy

Supported Exempt Accommodation

Version 1.0

Policy Control	
Policy Name	CCTV Policy – Supported Exempt Accommodation
Author	Chief Operating Officer
Policy Owner	Head of SEA / Tenant Support Services
Version No.	1.0
Approved by	Chief Operating Officer
Date of Implementation	01/04/2026
Date of Next Review	01/04/2028

Contents

1. Introduction and Purpose 3
2. Scope 3
3. Legislative and Regulatory Framework 4
4. Data Controller Status 4
5. Roles and Responsibilities 5
6. Description of the System 5
7. Siting of Cameras 6
8. Storage and Retention 6
9. Signage and Notification 7
10. Management and Access 7
11. Residents' Rights (Subject Access Requests) 8
12. Disclosure to Third Parties 8
13. Tenant Communication and Information Sharing 9
    13.1 Information to Residents 9
    13.2 Information to Managing Agents and Contractors 9
14. Incident and Data Breach Reporting 9
15. Safeguarding Considerations 9
16. Complaints and Appeals 10
17. Equality, Diversity and Inclusion 10
18. Policy Review 10
19. Related Policies and Documents 10

1. Introduction and Purpose

1.1 Reliance Social Housing CIC ("Reliance") is a Registered Provider regulated by the Regulator of Social Housing (RSH). Reliance manages a portfolio of Houses in Multiple Occupation (HMO) providing exempt supported accommodation for vulnerable homeless adults. These properties are managed on Reliance's behalf by a network of Managing Agents under Managing Agent Agreements.

1.2 Managing Agents at a number of Reliance properties have installed, or may wish to install, Closed Circuit Television ("CCTV") systems to support the safety and security of residents and the properties themselves. This policy sets out the governance framework within which CCTV must be procured, installed, operated and overseen at properties managed on Reliance's behalf.

1.3 Reliance does not itself install or operate CCTV systems. The responsibility for the day-to-day procurement, installation, operation and maintenance of CCTV at individual properties sits with the Managing Agent. However, as the Registered Provider and data controller, Reliance retains overall accountability for ensuring that any CCTV use at its properties is lawful, proportionate and aligned with its regulatory and safeguarding obligations.

1.4 The purpose of CCTV at Reliance properties is limited to:

- Safeguarding residents, particularly those at risk of harm, exploitation, or self-neglect
- Providing a safe and secure living environment for residents, staff, and visitors
- Supporting Managing Agents and support workers in managing incidents, including anti-social behaviour and emergencies
- Preventing and detecting crime
- Protecting buildings, assets, and communal areas
- Supporting investigations and partnership working with safeguarding agencies and law enforcement where necessary

1.5 CCTV must not be used to:

- Monitor residents' private lives unnecessarily
- Replace appropriate staffing or support provision
- Intrude into areas where individuals have a reasonable expectation of privacy

1.6 Reliance recognises that residents of its properties are vulnerable individuals who may be in crisis or transition. CCTV must therefore always be used proportionately, respectfully, and in a way that minimises intrusion into private life and is consistent with a trauma-informed approach.

2. Scope

2.1 This policy applies to all CCTV systems installed or operated at SEA properties regardless of whether the system was procured by Reliance or by the Managing Agent.

2.2 The policy applies to:

- All Managing Agents operating under a Managing Agent Agreement with Reliance
- Residents of Reliance properties
- All Reliance staff, including the Senior Leadership Team and Board of Directors
- Support workers, including those employed by commissioned providers
- Visitors, contractors, and external professionals

- Any individual whose image may be captured by a CCTV system at a Reliance property

2.3 This policy covers all fixed and movable camera systems, whether analogue or digital, including those operated remotely. It applies to both existing CCTV installations and any future installations.

2.4 Managing Agents are required to comply with this policy as a condition of the Managing Agent Agreement. A copy of this policy will be issued to all Managing Agents, and compliance will be monitored through Reliance's audit and performance review processes.

3. Legislative and Regulatory Framework

3.1 This policy is informed by and complies with the following legislation, statutory codes, and regulatory standards:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998, in particular Article 8 (right to respect for private and family life)
- Protection of Freedoms Act 2012, Part 2 (regulation of CCTV and other surveillance camera technology)
- Surveillance Camera Code of Practice (issued under Section 30 of the Protection of Freedoms Act 2012)
- Information Commissioner's Office (ICO) guidance on video surveillance, including the ICO CCTV Code of Practice
- Regulation of Investigatory Powers Act 2000 (RIPA), insofar as it applies to any directed or covert surveillance
- Regulator of Social Housing (RSH) Consumer Standards, in particular the Safety and Quality Standard
- Housing Act 2004 (management regulations applicable to HMOs)

3.2 Covert surveillance must not be conducted at any Reliance property unless expressly authorised under RIPA with appropriate legal advice and the written approval of the Chief Operating Officer. Any such authorisation must be time-limited, proportionate, and documented. Managing Agents have no authority to conduct or commission covert surveillance.

4. Data Controller Status

4.1 Reliance Social Housing CIC is the data controller for all personal data captured by CCTV systems at properties managed by Reliance, regardless of whether the CCTV system was procured or is operated by the Managing Agent.

4.2 Where a Managing Agent installs and operates CCTV at a Reliance property, that Managing Agent acts as a data processor on Reliance's behalf. The processing relationship, including obligations relating to security, access, retention, breach notification, and compliance with this policy, is governed by the Managing Agent Agreement and the associated Data Processing Agreement.

4.3 Where a Managing Agent operates CCTV systems at properties it manages independently of Reliance (i.e. properties not within Reliance's portfolio), the data controller status for those systems is a matter for the Managing Agent. This policy applies only to CCTV at properties managed by Reliance.

5. Roles and Responsibilities

5.1 The following roles carry specific responsibilities in relation to CCTV governance:

Role	Responsibilities
Board	Strategic oversight of CCTV governance across the Reliance portfolio. Receives assurance via COO reporting that CCTV operated by Managing Agents is lawful and proportionate. Approves this policy and any material changes to CCTV strategy.
Chief Operating Officer	Policy owner with overall accountability for CCTV governance. Ensures Managing Agent compliance with this policy via contractual obligations and audit. Authorises any extension of CCTV footage retention beyond the standard 30-day period. Escalation point for CCTV-related data breaches, complaints, or regulatory queries.
Head of SEA / Tenant Support Services	Issues corrective action notices to Managing Agents where non-compliance is identified.
Data Protection Officer (DPO)	Handles all Subject Access Requests relating to CCTV footage. Manages ICO notification in the event of a CCTV-related data breach. Advises on lawful basis, proportionality, and data sharing decisions. Authorises (jointly with COO) any disclosure of CCTV footage to third parties.
Managing Agents	Responsible for the procurement, installation, operation, and maintenance of CCTV systems at properties under their management, in accordance with this policy and the Managing Agent Agreement. Ensure CCTV signage meets the requirements of this policy at all relevant properties. Maintain local access logs and restrict access to authorised, trained personnel only. Inform residents of CCTV use at the point of move-in, as required by this policy. Ensure footage is retained and deleted in accordance with Section 10. Must not disclose footage to any third party, or respond to Subject Access Requests, without prior written authorisation from Reliance.
Support Workers (including commissioned providers)	Access CCTV footage only when expressly authorised by the Managing Agent or Reliance for a documented, legitimate purpose. Report any concerns about CCTV misuse, system faults, or data breaches to the Managing Agent and to Reliance.

6. Description of the System

6.1 CCTV systems installed by Managing Agents at Reliance properties may include:

- Fixed and/or movable cameras
- External cameras covering entrances, exits, and perimeters
- Internal cameras in communal areas only (hallways, stairwells, shared kitchens or lounges where justified)

6.2 Cameras must be connected to secure digital recording systems. Recording equipment must be located in restricted-access areas at each property and must not be accessible to residents or unauthorised visitors.

6.3 Audio recording must not be used unless strictly necessary, justified by a documented risk assessment, and approved by Reliance's DPO. Where audio recording is authorised, this must be clearly communicated to affected individuals via signage and privacy notices.

7. Siting of Cameras

7.1 Cameras must be positioned to support safeguarding and security purposes only. The positioning of every camera must be justified by a documented assessment of necessity and proportionality.

7.2 Cameras must be clearly visible and supported by signage that complies with the requirements set out in Section 11 of this policy.

7.3 Cameras must not be installed in:

- Bedrooms
- Bathrooms or toilets
- Private living spaces
- Any area where an individual has a reasonable expectation of privacy

7.4 Cameras may be installed in:

- Entrances and exits
- Hallways and stairwells
- Shared kitchens or lounges (where justified by a documented risk assessment)
- External areas including gardens, car parks, and perimeter boundaries

7.5 Special consideration must be given to:

- Residents' dignity, autonomy, and the principles of trauma-informed care
- Avoiding unnecessary or disproportionate surveillance of vulnerable individuals
- The potential for CCTV to cause distress, anxiety, or re-traumatisation

8. Storage and Retention

8.1 CCTV footage must be retained only for as long as is necessary for the purposes for which it was recorded.

8.2 The standard retention period is 30 days from the date of recording. At the expiry of 30 days, footage must be automatically overwritten or securely deleted by the Managing Agent.

8.3 Footage may be retained beyond 30 days only where:

- It is required for an active safeguarding investigation
- It is required for legal or criminal proceedings, or is subject to a preservation request from law enforcement
- It is the subject of a pending Subject Access Request
- Retention is expressly authorised in writing by the Chief Operating Officer, with documented justification

8.4 Managing Agents must ensure the following security measures are in place for CCTV storage:

- Password-protected access to recording systems, with individual credentials for each authorised user

- Encrypted storage where the system specification permits
- Restricted physical access to recording equipment
- Regular testing and maintenance of recording systems to ensure continuous operation

8.5 The Managing Agent is responsible for ensuring that the storage and deletion requirements of this policy are met at property level.

9. Signage and Notification

9.1 All properties with active CCTV systems must display clear, prominent signage at every point of entry to a surveilled area. The Managing Agent is responsible for procuring and installing signage.

9.2 Signage must comply with the ICO's guidance and the Surveillance Camera Code of Practice and must include, at minimum:

- The identity of the data controller (Reliance Social Housing CIC)
- The purpose of the CCTV surveillance
- Contact details for enquiries (Reliance's registered office address or a designated email address)
- A reference to the right to request access to footage (Subject Access Request)

9.3 Signage must be positioned at a height and in a location that is clearly readable by all individuals, including those with mobility or visual impairments.

10. Management and Access

10.1 The CCTV system at each property is managed on a day-to-day basis by the Managing Agent, subject to the requirements of this policy and the Managing Agent Agreement.

10.2 Access to live and recorded CCTV footage at property level is strictly limited to Managing Agent personnel.

10.3 Reliance retains the right to access CCTV footage at any Reliance property at any time. Access at Reliance level is limited to:

- The Chief Operating Officer
- The Head of SEA / Tenant Support
- Head of Community Liaison Officer Team
- The Data Protection Officer

10.4 Footage may be accessed only when there is a documented, legitimate reason, including:

- An active safeguarding concern
- A serious incident requiring investigation
- A criminal investigation (in conjunction with law enforcement)
- A Subject Access Request
- A complaint investigation
- A compliance audit

10.5 All access to CCTV footage must be logged by the Managing Agent. The access log must record:

- The date and time of access
- The identity of the person accessing the footage

- The reason for access, with reference to a specific incident, case, or request
- Whether any footage was copied, downloaded, or shared

10.6 Access logs must be available for inspection by Reliance at any time and will be reviewed as part of Reliance's periodic compliance audits.

10.7 Unauthorised access to, or misuse of, CCTV footage by Managing Agent personnel will be treated as a material breach of the Managing Agent Agreement. For Reliance staff, misuse will be treated as a disciplinary offence and may constitute gross misconduct.

11. Residents' Rights (Subject Access Requests)

11.1 Residents and any individuals captured on CCTV have the right to request access to footage in which they appear. Such requests are Subject Access Requests (SARs) under UK GDPR.

11.2 Managing Agents must not respond to SARs directly. All requests received at property level must be forwarded to Reliance's Data Protection Officer within two working days.

11.3 Reliance will respond to SARs within one calendar month of receipt, in accordance with UK GDPR Article 12.

11.4 Where footage includes other identifiable individuals:

- Images of third parties will be redacted (for example, by blurring or masking) before disclosure, unless consent has been obtained or disclosure is otherwise lawful
- Each disclosure decision will be assessed individually for fairness and legality

11.5 A record of all SARs received, the decision taken, and any footage disclosed will be maintained by the DPO.

12. Disclosure to Third Parties

12.1 CCTV footage must only be disclosed to third parties where there is a lawful basis to do so.

12.2 Managing Agents must not disclose CCTV footage to any third party without the prior written authorisation of Reliance. This includes disclosure to the police, local authority, or any other body.

12.3 Disclosure may be authorised by the COO or DPO to:

- Police or law enforcement agencies, where there is a lawful request or a legal obligation to disclose
- Local authority safeguarding teams, where disclosure is necessary for the protection of a vulnerable adult
- Courts, tribunals, or regulatory bodies, where disclosure is required by law or court order
- Insurers, where disclosure is necessary for the investigation or defence of a claim

12.4 All disclosures must be:

- Authorised by the COO or DPO
- Documented, including the identity of the recipient, the reason for disclosure, the footage disclosed, and the date
- Limited to the minimum footage necessary for the stated purpose
-

13. Tenant Communication and Information Sharing

13.1 Information to Residents

Residents must be informed about the use of CCTV at their property at the point of move-in. The Managing Agent is responsible for providing this information, which must include:

- A clear explanation of the purpose of CCTV and the areas covered
- Confirmation that cameras are not installed in private areas
- The identity of the data controller (Reliance Social Housing CIC)
- Information on how to make a Subject Access Request
- Information on how to raise concerns or complaints about CCTV use

This information should be provided in an accessible format and communicated sensitively, taking account of residents' vulnerabilities, language needs and any trauma-informed considerations.

13.2 Information to Managing Agents and Contractors

Managing Agents are provided with a copy of this policy and are required to operate CCTV in accordance with its requirements as a condition of the Managing Agent Agreement. Contractors and other third parties attending Reliance properties must be made aware that CCTV is in operation via the signage required under Section 9.

14. Incident and Data Breach Reporting

14.1 Any incident involving CCTV at a Reliance property, including unauthorised access, system failure, loss of footage, or a suspected data breach, must be reported as follows:

- The Managing Agent must report to Reliance's Head of Property Compliance and the DPO within 24 hours of becoming aware of the incident
- Reliance staff who become aware of a CCTV-related incident must report to their line manager and the DPO within 24 hours

14.2 Where a data breach involving CCTV footage meets the threshold for notification under UK GDPR Article 33 (i.e. it poses a risk to the rights and freedoms of individuals), the DPO will notify the Information Commissioner's Office within 72 hours of Reliance becoming aware of the breach.

14.3 Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals, those individuals will be notified directly in accordance with UK GDPR Article 34.

14.4 All CCTV-related incidents and data breaches will be recorded on Reliance's incident log and reported to the COO. Lessons learned will be incorporated into policy reviews and Managing Agent communications as appropriate.

14.5 Failure by a Managing Agent to report a CCTV-related incident within the required timeframe will be treated as a material breach of the Managing Agent Agreement.

15. Safeguarding Considerations

15.1 Reliance's properties provide supported accommodation for vulnerable homeless adults. The use of CCTV in this context requires particular sensitivity, and Managing Agents must exercise this in their day-to-day operation of CCTV systems.

15.2 CCTV must support safeguarding objectives. It must not replace the provision of appropriate staffing, support, or care. Managing Agents and support workers must prioritise

direct engagement, relationship-building, and trauma-informed intervention over reliance on surveillance technology.

15.3 Surveillance must not create an environment of distress, mistrust, or control. Where a resident raises concerns about CCTV, these must be taken seriously by the Managing Agent, recorded, and escalated to Reliance if they cannot be resolved at property level.

15.4 Where CCTV footage reveals a safeguarding concern, this must be escalated immediately through Reliance's safeguarding procedures, regardless of the original reason for accessing the footage.

16. Complaints and Appeals

16.1 Any individual who wishes to raise a concern or complaint about the use of CCTV at a Reliance property may do so through Reliance's Complaints Policy.

16.2 Residents will be supported to raise concerns where needed, including through advocacy services where appropriate.

16.3 Complaints relating to data protection rights (including the handling of Subject Access Requests) may also be referred to the Information Commissioner's Office.

17. Equality, Diversity and Inclusion

17.1 Reliance is committed to ensuring that the operation of CCTV at its properties does not disproportionately or unfairly impact any individual or group on the basis of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation.

17.2 This policy has been assessed for its equality impact and will be kept under review to ensure it remains compliant with the Equality Act 2010 and Reliance's Equality, Diversity and Inclusion Policy.

18. Policy Review

18.1 This policy will be reviewed every 2 years, or sooner if:

- Relevant legislation, statutory codes or regulatory standards are updated
- There is a material change to Reliance's operating model, portfolio or Managing Agent network
- A significant CCTV-related incident, complaint, or regulatory finding occurs
- The Regulator of Social Housing issues guidance relevant to CCTV or surveillance

18.2 The policy owner (Chief Operating Officer) is responsible for commissioning the review and approval for any material amendments.

19. Related Policies and Documents

- Data Protection Policy
- Safeguarding Policy
- Health and Safety Policy
- Complaints Policy
- Equality, Diversity and Inclusion Policy
- Managing Agent Agreement
- Incident Reporting Policy