

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

CLOSED CIRCUIT TELEVISION (CCTV) POLICY

Author	Data Governance Manager
Contributors	Governance team, external GDPR consultant, Senior Management Team, Executive Leadership Team
Review Frequency	3 years
Latest Review Date	April 2025
Approved By & Date	Executive Director, Governance and Compliance May 2025
Next Review Date	May 2028

Contents

	Page No.
1. Policy purpose & aim	3
2. Objectives	3
3. Scope of policy	3
4. Responsibilities	3
5. Monitoring & review	5
6. Risk management	5
7. Statement of commitment	6
8. Additional Arrangements - CCTV	7
8.1 Why we have CCTV	7
8.2 Overt versus covert CCTV	8
8.3 Location and installation of CCTV	8
8.4 Signage	9
8.5 Data Protection Act /GDPR and review of existing systems	9
8.6 Monitoring of CCTV	10

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

	8.7 Retention period for CCTV images/footage	11
	8.8 CCTV system maintenance	11
	8.9 CCTV system training	11
	8.10 Access to footage	11
	8.11 Disclosing images/footage	12
	8.12 CCTV Subject Access Requests	14
	8.13 Complaints Procedure	14
9. Other relevant ExtraCare policies & documents		14
10. Relevant legislative & regulatory requirements		15

Version Control

Version	Date	Description	Updated By	Approved By
1.0	06.09.17	First draft	Governance & Risk Officer	December 2018
2.0	December 2021	Review following input from GDPR consultant. Move to new policy format. Revisit of content e.g., resident access basis for legitimate interest.	DoG&C	ELT February 2022
2.1	May 2022	Review date amended to February 2025	Governance & Risk Officer	Compliance & Risk Manager
2.2	August 2024	Update to section 8.6	Compliance Manager	Executive Director, Governance and Compliance
3.0	May 2025	Update to section 8.12; responsibility to ensure CCTV checklists are in place/reviewed re-assigned to the Data Governance Manager; addition of Staff Work Instructions to support this policy. Update to 8.8 data security expectations under contract with supplier	Data Governance Manager	Executive Director, Governance and Compliance

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

1. Policy Purpose & Aim

The ExtraCare Charitable Trust (ExtraCare) is committed to providing a safe environment for its staff, residents, volunteers, and visitors. To facilitate this, ExtraCare has a comprehensive and overt closed-circuit television (CCTV) surveillance system at its locations for the purposes set out below. The purpose of this policy is to provide clarity on the operation of CCTV systems and the approach to be adopted when a request is received to view captured images either as a result of an incident occurring or a data subject access request.

2. Objectives

The objectives of this policy are to ensure that:

- There is a consistent approach to the installation and use of CCTV across all locations;
- Use of CCTV meets the requirements of data protection law, human rights, and other relevant legislation;
- The rights of all individuals who may have their personal data recorded are protected and respected;
- CCTV systems are operated effectively, and efficiently and are not open to abuse; and
- Understanding exists about how CCTV is be used.

3. Scope of Policy

This policy applies to all use of CCTV operated by ExtraCare on its premises including schemes, villages, Head Office and within the Retail subsidiary. This policy does not cover CCTV owned by residents.

4. Responsibilities

Executive Director Governance & Compliance	Approve the policy.
Asset Owner (Assets Investment Manager)	Responsible for ensuring there is a maintenance contract in place with the vendor which meets the requirements of the IT Cyber Security Policy.

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

	Monitor requests for repairs and new requests to ensure they are carried out within the terms of the agreement. Consult with appropriate responsible areas of the business regarding requests for additional CCTV.
Development/Commissioning Team (Head of Development/Head of Special Projects)	Ensure that new CCTV installations, for developments, modernisations, and extensions, have clear contracts in place and are subject to a privacy impact assessment (including both the use and positioning of CCTV and location for viewing of images). Consult with Operations to ensure clarity on who the responsible local manager for CCTV is in such instances. Consult with IT with respect to security/connectivity.
Regional Operations Managers	Ensure that the schemes/villages have a nominated responsible manager for CCTV and that the responsible manager discharges their responsibilities.
Responsible local manager for CCTV	Each location with CCTV will have a nominated responsible manager. • For schemes/villages – this is the location manager • For Head Office – this is the Asset & Maintenance Manager • For Retail – this is the Regional Manager Responsibilities include: • Ensure that changes/new installations are subject to a privacy impact assessment. • Ensuring appropriate signage is in place. • Limiting access and ensuring sharing and retention of data is in line with this policy. • Ensuring users of CCTV at locations are suitably trained and local procedure notes held. • Ensure CCTV systems are maintained. • Ensure the IT Service Desk is notified before any cameras or CCTV devices are moved or added. • Ensure that existing CCTV at locations is subject to a periodic check every 2 years (see Work Instruction 1). • Ensure records are held where CCTV has been accessed.

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

	• Ensure records are held of any CCTV disclosures. • Ensure that the Data Protection Officer (DPO) is consulted before sharing CCTV (or is notified afterwards in the event of an emergency).
Data Governance Manager (Data Protection)	Review/update this policy. Amend to reflect changes, learnings, or in response to incidents/queries. Ensure CCTV System Review Checklists are in place at all locations and undertake period checks/audits. Provide advice. Seek advice e.g. from Data Protection Officer/legal advisors.
All	Adhere to this policy.

5. Monitoring & Review

The success of this policy in delivering its aims and ensuring that ExtraCare complies with relevant legislation will be monitored. Policy effectiveness will be assessed through the volume and nature of queries received and periodic audits of the checklist included in the CCTV Work Instruction. This policy will be subject to a full review at least every 3 years.

All images processed by ExtraCare CCTV systems (including at the subsidiary) will remain the property and copyright of ExtraCare, although in some cases we may allow others to see or obtain copies of the footage.

6. Risk Management

The Board of Trustees have set a minimalist risk appetite for legislative and regulatory risk as this represents both a significant financial and reputational risk for ExtraCare. Compliance with this policy and related documents reduces the risk of a breach in relation to use of CCTV and supports ExtraCare to meet its legislative and regulatory obligations.

Images of individuals captured by CCTV are classed as personal data/information and are therefore subject to data protection law. This policy should be applied in conjunction with the Data Protection Policy. Images captured by CCTV and records relating to the installation, maintenance and use of the systems are ExtraCare records and must be managed in accordance with the Records Management Policy. Breaches of this policy may result in data protection or information security breaches and could

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

result in disciplinary action. Any suspected breach or incident should be reported in accordance with the Data Protection Policy.

The misuse of CCTV may be regarded as a breach of the Data Protection Act and in some circumstances a criminal offence and if, following investigation, it is found that CCTV has been used for any other purpose other than for that which it is intended, ExtraCare may report cases to the appropriate authorities. Any member of staff found to be misusing CCTV may be subject to disciplinary proceedings. Appropriate action may also be taken against any resident found to be using the CCTV for purposes other than those permitted and set out in this policy.

7. Statement of Commitment

We want to ensure that our staff, residents, volunteers, and visitors to our locations feel safe and secure. It is ExtraCare's policy to operate CCTV at its locations in order to help reduce the fear of crime and provide reassurance to everyone who accesses our locations. ExtraCare has notified its use of CCTV to the Information Commissioner's Office (ICO) and will continue to meet ICO requirements. Although we are not subject to regulation by the Surveillance Camera Commissioner, we will have regard to the *12 guiding principles of the Surveillance Camera Code of Practice (source: Biometrics and Surveillance Camera Commissioner, updated January 2021)*:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need;
2. The user of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified;
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints;
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, and used;
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them (*this policy*);
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged;
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes;

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards;
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use;
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published;
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value; and
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

8. Additional arrangements - CCTV

8.1 Why we have CCTV

CCTV may be installed to:

- Create a safer environment for our residents, staff, volunteers, and visitors;
- Help assist in the prevention and detection of crime against both persons and property and prevent and respond effectively to all forms of disorder;
- Help reduce the fear of crime for residents, staff, and visitors, particularly for those entering or leaving the premises during the hours of darkness;
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime committed at our locations;
- Assist in the investigation of any suspected breaches of regulations/ relevant codes of conduct ExtraCare or its, employees, officers, agents, or contractors are subject to;
- Gather evidence by a fair and accountable method;
- Provide emergency services assistance;
- Assist with health and safety and other serious occurrences;
- Detect, prevent, and reduce the incidence of any internal conduct and performance matters which can lead to disciplinary procedures being initiated; and
- Assist in the investigation of any claims including, but not limited to, Public Liability or Road Traffic Accident-related matters.

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

8.2 Overt versus covert CCTV

Overt CCTV surveillance is where cameras are on open display and there are signs around the building advertising their use.

Covert surveillance is when the CCTV cameras are not advertised, are hidden from view and images are captured without the knowledge of individuals.

Covert surveillance (when the CCTV cameras are hidden, operated without the knowledge of residents, staff, or visitors) is **not** generally conducted. However, ExtraCare reserves the right to use covert surveillance in certain circumstances, subject to the completion of a Data Protection Impact Assessment (DPIA). In making any decision to use covert surveillance we will take account of Home Office guidance on covert surveillance produced under the Regulation of Investigatory Powers Act 2000 ('RIPA') as a matter of good practice, although we are not a public authority for the purposes of RIPA. If directed covert surveillance is required, this must be authorised in writing by the Executive Director (Corporate Resources) and DPO.

8.3 Location and installation of CCTV

Using surveillance systems can be privacy intrusive. Careful consideration should therefore be given before any new installation (including use of Automatic Number Plate Recognition systems), and use should be for a specified purpose/to address a specific issue. Consideration should consider the nature of the problem; whether CCTV is a justified/effective solution; whether better solutions might exist; the effect on individuals; and whether therefore CCTV is a proportionate response to the problem. This assessment is a **Data Protection Impact Assessment ('DPIA')**.

This assessment must be completed in every instance e.g., installation at a new location; new installation at an existing location; or a replacement of equipment (e.g. through modernisations/update of technology). Responsibility for ensuring that this assessment is undertaken rests with relevant 'responsible local manager' as defined in Section 4.

Example – CCTV is considered to alleviate safety concerns in a dark car park. An alternative solution which is less privacy intrusive is to install improved lighting.

In general, CCTV cameras are installed to cover entrances to the premises, car parks and reception areas. Other areas have been protected on a location-by-location basis dependant on consideration of specific risks (e.g., safe rooms). As a general principle, cameras will be positioned to avoid impinging on the privacy of individuals not visiting the premises and considering legislative requirements and published guidance.

In new village locations, CCTV will be installed to cover the following areas:

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

- Premises' entrances and exits;
- Car parks; and
- Reception and communal areas.

Changes or extensions to this CCTV basic coverage as outlined above will be subject to completion of a DPIA – this assessment will be performed before any CCTV is installed.

Any movement of existing, or installation of additional cameras or devices should be notified to the IT Service Desk to validate the correct network connectivity is used. All CCTV system must be under a maintenance contract that meets the requirements IT Cyber Security Policy. Specifically, all network attached devices must be regularly updated with the latest software and security patches must be applied within 14 days of issue by the vendor.

8.4 Signage

All locations using CCTV will have signage. As far as possible, cameras will be clearly visible and clear, readable signage will be prominently displayed advising that CCTV cameras are in operation. Signs will be displayed in relevant locations and should give people notice before/at the same time as they are filmed on CCTV. This means that CCTV notices are required in car parks, at doorways (before entering the premises) and within premises. Such signs will indicate:

- The presence of monitoring and recording;
- The ownership of the system (Data Controller);
- How to contact ExtraCare for more information (to enable the data subject to exercise their rights under applicable data protection laws). This should be Reception of the respective location in the first instance.

8.5 Data Protection Act/GDPR and review of existing systems

The collection, use and storage of personal data is governed by Data Protection legislation including, but not limited to the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR). ExtraCare is registered with the ICO as a data controller operating CCTV.

Given that a CCTV recording may include personal data; all such recordings will be treated in accordance with the data protection principles under relevant data protection legislation and in accordance with our Privacy Policy, which is available from ExtraCare's website.

Data subjects' rights, including access to their personal data will be respected where recordings are confirmed to comprise personal data. Where an individual requests access to recordings believed to

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

be their personal data, the matter shall be referred to the Data Protection Officer (DPO) to be dealt with in accordance with a subject access request. If the DPO deems that the request is valid, as far as possible third-party data will be removed before a Subject Access Request will be fulfilled. If, for whatever reason, it is not possible to remove third party images and it would not be reasonable to disclose the footage without the consent of those third parties, we may refuse to disclose footage.

A review of existing systems will be undertaken at least every three years as this policy is updated to ensure use remains valid. **See Work Instruction 1 – Existing CCTV System Review Checklist.** Records will be held at each location using CCTV and be available for audit. Any issues arising will be notified to the Regional Operations Manager (for schemes and villages) and reported to the DPO via privacy@extracare.org.uk (in all instances).

8.6 Monitoring of CCTV

Routine and regular monitoring of live or recorded CCTV will only take place at locations where night security (or concierge service) is in place. This will specifically cover car parks or integral external areas, for the purpose of alleviating concerns and in the prevention or identification of crime.

Equipment will only be used by night staff who have been authorised by the Location Manager as the nominated responsible manager for CCTV (see Section 4 - Responsibilities) to do so using secure log on details.

In all other circumstances there will not be routine monitoring of live or recorded CCTV. Images will only be viewed should an incident occur, as an aid to the detection or prevention of crime, and to facilitate the identification, apprehension, and prosecution of offenders.

Viewing of recorded images will only be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised personnel (an employee or appointed person (e.g., camera installation or repair contractor) acting on behalf of ExtraCare who has an operational responsibility for the security and safety of a location's premises).

Residents in certain locations have access to limited CCTV live footage (See section 8.11).

8.7 Retention period for CCTV images/footage

Images will not be stored for longer than is necessary. This is usually 28 days (and no longer than 30 days). CCTV systems should be configured to overwrite data every 28 days (or a maximum of 30 days) to ensure excessive data is not retained. If systems do not automatically overwrite data, then the responsible local manager will ensure data is deleted after 30 days.

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

In the event of the recorded image being required by law, for evidence or the investigation of crime, it will be retained for a period of time required by law or until it is no longer required for evidential purposes, or any investigation has been completed. The rationale for this shall be recorded.

8.8 CCTV System Maintenance

CCTV systems will be subject to regular maintenance to ensure that the system is working properly and produces high quality images with correct date/time.

At any update/replacement a full DPIA will be undertaken to ensure that CCTV remains the most appropriate solution to the problem sought to be solved.

In most locations CCTV cameras and devices are isolated on separate and dedicated computer networks to enhance information security. All CCTV system must be under a maintenance contract that meets the requirements IT Cyber Security Policy. Specifically, all network attached devices must be regularly updated with the latest software and security patches must be applied within 14 days of issue by the vendor.

8.9 CCTV System Training

ExtraCare will ensure that managers (or relevant designated staff) who are responsible for CCTV at their location understand how the system works, what it covers, how to view recorded images and delete data (if this is not erased automatically after 30 days), and how to extract images from the system when required.

Training on use of the CCTV system will form part of induction training for nominated staff with additional/top-up training provided as/where required by the responsible location manager This training will include awareness and understanding of this policy.

See Work Instruction 2 - CCTV Staff Instructions

Local training notes/procedures will be held on use/navigation of the CCTV system by the responsible location manager

8.10 Access to footage

Access to CCTV will be limited to authorised personnel only (see 8.6 above), as determined by the responsible local manager, and must be in accordance with the stated purposes of the system.

Access will be within a self-contained room in the building with controlled access where only authorised personnel will be granted permission (e.g., not viewable an open office/behind reception).

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

At some locations, the CCTV system will enable staff to view persons waiting for entry into the location through their communication handset (where resident call / entry phone system offers this capability).

A record of all people who have accessed will be maintained at each site. This will be regularly reviewed by the responsible local manager.

Access to live streamed CCTV footage will also be available on a limited basis to residents in their apartments (see section 8.11).

8.11 Disclosing Images/Footage

The responsible local manager may permit the viewing of CCTV recorded material to the police and other third parties where this is necessary in connection with an incident captured on the CCTV. ExtraCare will only disclose CCTV images for the purpose for which it was collected, as detailed in section 8.1 of this policy.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser, and reason for the disclosure.

Where necessary, ExtraCare may disclose images to a third party (including, but not limited to the Police or any other relevant authority/governing body), such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where there is justification or where an exemption applies under relevant legislation (including, but not limited to, in connection with legal proceedings).

A request for copies of images by a third party must be submitted to the DPO via privacy@extracare.org.uk, at the earliest opportunity. The request will then be considered by the DPO, the Legal Manager, and/or Compliance & Risk Manager (on behalf of the DPO). The final decision as to whether images will be disclosed will rest with the DPO.

In the event of an emergency/out of hours request where the DPO is not available and the request is urgent and from a relevant authority/governing body (e.g., the Police), the responsible local manager or senior manager on-call is permitted to respond to the request providing that:

- the relevant authority/governing body has provided sufficient identification and confirmation of the purpose of the request (including under which legislation they are requesting it);
- the CCTV/information/ documentation is only provided to the relevant authority/governing body, it is limited to what is necessary to satisfy the request and it can and will be shared securely;
- all data files (images, video) are transmitted or sent to third parties in a secure manner (e.g. encrypted with password sent separately, by tracked courier) and compliant with IT Security Policy; and

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

- the DPO is notified immediately by email (to privacy@extracare.org.uk) of what has been shared with the relevant authority/ governing body, what identification they provided and what the purpose of the request was.

HR investigations - Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/Advisor, the DPO may agree access to CCTV images.

Resident access

In some villages, residents are provided with limited access to CCTV footage from their apartments. This is for security purposes in order that residents feel safe and can grant access to visitors to the village and/or their apartment outside of the working day when the main reception has closed. Mitigations are in place as resident's access to CCTV footage should be limited to:

- Main entrance(s) / exit(s) to the village/scheme;
- Internal entrance(s) / exit(s) to the village/scheme residential areas
- Certain times of the day i.e., between 5pm and 8am Mon-Fri and 24hrs at the weekend (i.e. outside of the normal working day) *where technologically possible*;

All such residents are prohibited from copying, modifying, or sharing the footage and are provided with the Permitted use notice that sets out all prohibited actions.

In order to share personal data under relevant data protection legislation (GDPR), this must be necessary for the purposes of our legitimate interests and such interests must be balanced with the interests, rights, and freedoms of any data subjects. ExtraCare will conduct a Legitimate Interest Assessment which it will conduct under the same criteria as the DPIA (see 8.3 and 8.8 above) to ensure it remains satisfied that there is a legitimate interest to permit residents to view limited CCTV footage of the areas specified above. This is to ensure that our residents feel safe in their own homes and in order for them to be able to prevent and detect unauthorised access and/or crime. This is particularly important given that locations do not have 24hr security and the location reception is generally closed and un-staffed during out-of-office hours and at weekends.

All residents with access to CCTV footage are provided with strict permitted use notices, which informs them that the CCTV is only to be viewed for the purpose of the prevention and detection of crime, and they are strictly forbidden from copying, recording, and/or sharing any footage with third parties. CCTV footage which is accessible to residents must not be recorded and can only be viewed live. Misuse of the system by a resident may result in access being removed or further action being taken.

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

8.12 CCTV Subject Access Requests (SARs)

Images of individuals captured on CCTV is personal information and individuals have rights in relation to their personal information, including a right of access. Further details of individual's rights are set out in ExtraCare's Privacy Policy available at www.extracare.org.uk.

Requests by individual data subjects for images relating to themselves are Subject Access Requests (SARs) and should be treated in accordance with the Data Protection Policy. These will be considered on a case-by-case basis in accordance with relevant data protection laws. The Data Protection Team will maintain records of CCTV SARs.

When a location receives a request from an individual data subject (either in writing (e.g. by email, letter or via social media) or verbally), the Work Instruction 'Subject Access Request Procedure – All Staff' should be consulted and the correct procedure followed.

8.13 Complaints Procedure

Any complaint concerning misuse of its CCTV system should follow the Complaints Policy.

9. Other Relevant ExtraCare Policies & Documents

General	• Data Protection Impact Assessments
Related Policies	• Data Protection Policy • Information Security Policy • Records Management Policy • Privacy Policy (Customer) • Employee Privacy Policy • IT Security Policy
Work Instructions	• Existing CCTV Systems Review Checklist • CCTV Work Instructions

10. Relevant Legislative & Regulatory Requirements

Legislation	Regulation	Guidance
UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18)		Data protection impact assessments guidance for conducting a data protection impact assessment on surveillance camera systems (2018)

Policy Name	CCTV
Version No.	3.0
Approval Date	May 2025
Category	Operational
Classification	Internal

Human Rights Act 1998		Surveillance Camera Code of Practice 2013 (issued under Section 30(1)(a) Protection of Freedoms Act 2012) updated 2022
Investigatory Powers Act 2016 (good practice in the context of ExtraCare's activities)		
Protection of Freedoms Act 2012 and associated Code of Practice (good practice in the context of ExtraCare's activities)		