Closed Circuit Television (CCTV)

Lead Director: Annette Brandwood

Reference: POL 83

Committee Review: N/A

SMT Approval: 27/11/25

Review Date: November 2028

1. Introduction & Aim

This Policy applies to all fixed and mobile Closed Circuit Television (CCTV) systems operated by Cobalt across its residential, commercial and operational sites.

The aim of this Policy is to establish a clear framework for the responsible, proportionate, and lawful use CCTV systems to:

- promote the safety and security of staff, customers, visitors and property
- deter and detect criminal activity, anti-social behaviour, and unauthorised access
- support the investigation of incidents and assist law enforcement where appropriate
- monitor operational procedures to ensure compliance and safety.

Cobalt is committed to ensuring that all CCTV operations comply with relevant legal and regulatory requirements, including UK General Data Protection Regulation, the Data Protection Act 2018, and the Surveillance Code of Practice. Cobalt recognises the importance of safeguarding individual privacy rights and will ensure that CCTV use is transparent, justified, and respectful of those rights at all times.

2. Policy Statement

This Policy outlines the purpose, scope, and management of CCTV systems operated by Cobalt. It applies to all employees, contractors, residents, customers and visitors within premises where CCTV is installed and operated by Cobalt.

CCTV systems will be used solely for legitimate purposes aligned with Cobalt's operational, safety, and legal obligations. All data captured through CCTV will be processed in accordance with applicable data protection laws and access to footage will be strictly controlled to prevent misuse or unauthorised disclosure.

3. Policy Principles

3.1 Lawful Basis for Installation, Article 6 of UK GDPR

Cobalt will deploy CCTV systems in appropriate areas across its operations, ensuring that their use is lawful, necessary and proportionate. As the designated Data Controller, Cobalt is responsible for the processing of images, footage, and any other personal data captured by these systems.

The lawful basis for processing CCTV data is established under Article 6(1)(f) of the UK General Data Protection Regulation (UK GDPR) — processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the rights and freedoms of the data subjects.

Cobalt systems will be operated solely in pursuit of the following legitimate aims:

- to deter and detect crime, vandalism, and unauthorised access.
- to enhance the safety and security of staff, customers, visitors and property
- to assist in the investigation of incidents and support law enforcement.
- to monitor operational and safety procedures for compliance and improvement.

Prior to the installation of any new CCTV system, Cobalt will conduct a Data Protection Impact Assessment (DPIA) to evaluate potential risks to individuals' rights and freedoms. This assessment will ensure that

appropriate safeguards are in place, and that the deployment of CCTV is justified, transparent, and aligned with data protection principles.

3.2 **Exemptions**

To safeguard individual privacy and ensure compliance with data protection legislation, Cobalt will not use CCTV systems for the following purposes:

- Audio Recording: CCTV systems will not be used to capture or record sound under any circumstances.
- Live Streaming: Footage will not be streamed live to the internet or used for commercial purposes.
- Monitoring Private Areas: Cameras will not be installed or used in private spaces such as restrooms, breakrooms, or other areas where individuals have a reasonable expectation of privacy

These exemptions reflect Cobalt's commitment to proportionality, transparency, and respect for the rights and freedoms of individuals.

3.3 **Operational Management of CCTV Systems**

Cobalt will ensure that all CCTV systems are managed securely, ethically, and in compliance with applicable data protection legislation. Physical and digital access to CCTV systems will be restricted to authorised personnel based on their roles and responsibilities.

Access Control
Access to CCTV equipment, footage, and related systems will be limited to designated staff with a legitimate business need. Role-based permissions will be enforced to prevent unauthorised access or misuse.

Role	**Key Responsibilities**
Assurance and Business Improvement Manager (Data Protection Coordinator)	• Advise on system functionality to ensure compliance with UK GDPR and the Surveillance Camera Code of Practice • Ensure signage is clearly visible, readable, and accessible (e.g. visual icons for language and literacy support) • Manage internal and external data access requests, ensuring proper disclosure protocols and audit trails (see sections 3.5 and 3.6) • Investigate privacy concerns, breaches, and complaints related to CCTV • Implement privacy masking to exclude irrelevant or sensitive zones from recording
Health and Safety Manager	• Access footage for health and safety incidents in accordance with approval protocols (see sections 3.5 and 3.6) • Ensure strategic camera placement in public areas, entrances, exits, and interview rooms • Oversee daily operation of CCTV systems • Monitor camera functionality and secure footage storage • Liaise with suppliers for system maintenance and service scheduling
Internet, Network and Security Manager	• Ensure footage is stored on secure servers or encrypted devices with restricted access

	• Enforce secure login credentials and multi-factor authentication for system access • Encrypt and log all data transfers (e.g. for backup or disclosure) • Conduct regular security audits and vulnerability assessments • Monitor system activity and advise on security functionality to prevent breaches and ensure compliance

3.4 **Data Retention**

Cobalt will retain CCTV footage only for as long as necessary to fulfil its legitimate purposes, in accordance with data protection legislation and internal retention schedules.

- **Standard Retention Period:** CCTV footage will be retained for a maximum of 30 calendar days from the date of recording.
- **Extended Retention:** Footage required for internal investigations, disciplinary actions, or law enforcement requests may be retained beyond the standard period. In such cases, a documented justification must be recorded, and retention will be reviewed periodically.
- **Secure Deletion:** After the applicable retention period, footage will be automatically and securely deleted or overwritten using system functionality designed to prevent recovery or unauthorised access.

Retention practices will be regularly reviewed to ensure compliance with the principles of data minimisation and storage limitation under UK GDPR.

3.5 **Subject Access Requests**

Under the UK GDPR, individuals (including employees, customers, visitors, and members of the public) have the right to request access to CCTV footage in which they are identifiable.

All subject access requests will be managed in accordance with Cobalt Subject Access Request Procedure.

How to Submit a Request

- Requests must be submitted in writing to the Cobalt Data Protection Coordinator.
- The request should include sufficient detail to identify the relevant footage (e.g. date, time, location, and description of the incident).

Grounds for Restriction or Refusal

Access to footage may be restricted or denied if:

- The footage contains third parties who cannot be anonymised without disproportionate effort.
- Disclosure would compromise an ongoing investigation or legal proceeding.
- The request is manifestly unfounded or excessive, particularly if repetitive or abusive.

Response Timeframe

Cobalt will respond to all valid subject access requests within one calendar month of receipt. In complex cases, this period may be extended by up to two additional months, with written notification and justification provided to the requester.

3.6 **Data Sharing Protocols**

CCTV footage may be shared with third parties only where such disclosure is lawful, necessary, and proportionate, and in accordance with data protection legislation and Cobalt's internal privacy policies. This includes, but is not limited to:

- Law enforcement investigations
- Legal proceedings
- Regulatory or statutory obligations

All disclosures must be authorised by the Data Protection Coordinator and will be subject to appropriate safeguards, including formal Data Sharing Agreements or documented legal requests were applicable.

Request Requirements
Requests for CCTV footage must:

- Be submitted in writing
- Clearly state the purpose of the request
- Specify the date, time, and location of the footage sought
- Identify the legal authority or justification for the request

Assessment and Approval
Each request will be assessed on a case-by-case basis to ensure:

- The request is lawful and proportionate
- Disclosure is necessary for the stated purpose
- The rights and freedoms of individuals captured in the footage are appropriately protected

Where disclosure is approved, footage may be shared securely with law enforcement agencies or other authorised bodies. All disclosures will be logged and auditable, and footage will only be retained for as long as necessary to fulfil the purpose of the request.

3.7 **Internal Investigation Requests**

CCTV footage may be reviewed and used as part of internal investigations where such use is necessary, proportionate, and justified. This includes, but is not limited to, investigations relating to:

- **People Team Matters**: Inquiries into employee conduct, safeguarding concerns, or workplace disputes where visual evidence may assist in establishing facts.
- **Health and Safety Incidents**: Analysis of accidents, near misses, or breaches of safety protocols, to improve future risk management and compliance.
- **Anti-Social Behaviour (ASB)**: Identification and resolution of incidents involving nuisance, harassment, or disorderly conduct affecting staff, customers, residents, or visitors.
- **Tenancy Breaches**: Investigation of suspected violations of tenancy agreements, including unauthorised occupancy, property damage, or behaviour that undermines community standards.

Request Procedure

Requests to access CCTV footage for internal investigations must follow the principles outlined in 3.5 and be submitted to the Cobalt Data Protection Coordinator for written approval.

To initiate a request, the following steps must be completed:

1. Complete the request proforma QR 004 - 'Request to View and/or Copy CCTV Footage', available in Cobalt's Document Library.
2. Submit the completed form via email to dataprotection@cobalthousing.org.uk including:
    - Date, time, and location of the incident
    - Purpose of the request
    - Names of individuals who will view the footage
    - Whether a copy of the footage is required
    - Whether the footage will be shared with a third party

Access and Audit

If access is granted by the Data Protection Coordinator:

- footage may be provided in a secure digital format or viewed in a controlled environment
- all requests, approvals, and disclosures will be logged and retained for audit and compliance purposes.

Third-Party Access

Where third-party service providers are engaged to install, maintain or operate CCTV systems on behalf of Cobalt, Cobalt will ensure that appropriate safeguards are in place to protect personal data.

- All third-party providers will be subject to a formal Data Processing Agreement (DPA) that outlines their responsibilities, limitations, and obligations under UK GDPR.
- The DPA will specify the scope of processing, data security measures, access controls, and breach notification procedures.
- Cobalt will conduct due diligence and periodic reviews of third-party compliance to ensure that personal data is handled lawfully, securely, and in accordance with the Policy.

No third-party shall access or process CCTV footage without explicit authorisation and a valid contractual basis.

3.8 **Data Breaches**

Cobalt takes the security and integrity of CCTV data seriously. Any suspected or confirmed data breach involving CCTV footage must be reported immediately to the Data Protection Coordinator and/or the ICT Security Team.

Upon notification, the appropriate team will:

- assess the nature and severity of the breach
- implement containment and mitigation measures
- notify affected individuals where required
- report the breach to the Information Commissioner's Office (ICO) if it meets the threshold for mandatory reporting.

All breaches will be managed in accordance with Cobalt's Data Breach Response Procedures, and appropriate disciplinary or remedial actions will be taken where necessary.

Examples of CCTV-Related Data Breaches

- **Unauthorised Access:** Viewing or accessing CCTV footage without a legitimate business reason or proper authorisation. Such actions will be treated as a serious breach and may result in disciplinary action.
- **Footage Leak:** Sharing CCTV footage externally (e.g., on social media or with the press) without lawful justification or consent.
- **Loss or Theft of Equipment:** Misplacement or theft of devices containing CCTV footage, such as DVRs or hard drives.
- **Hacking or Malware Attack:** Cyber-attacks that compromise CCTV systems and result in unauthorised access or data loss.
- **Improper Disclosure:** Sharing footage with third parties (e.g., law enforcement, insurers) without following proper legal or internal procedures.
- **Failure to Delete:** Retaining footage beyond the approved retention period without justification or approval.
- **Insecure Transmission:** Transferring footage via unencrypted channels or storing it on unsecured devices.

Training and Awareness

All staff with access to CCTV systems will receive regular training to ensure they understand:

- their responsibilities under UK GDPR and the Data Protection Act 2018
- the appropriate and lawful use of CCTV systems
- the rights of individuals whose data is captured
- procedures for handling access requests, disclosures, and breaches.

Training will be refreshed periodically and documented as part of Cobalt's ongoing commitment to data protection and privacy compliance.

Monitoring and Review

The Data Protection Coordinator will conduct periodic audits of CCTV operations to ensure compliance with this Policy, data protection legislation, and the Surveillance Camera Code of Practice.

This Policy will be reviewed every three years or sooner if there are significant changes in legislation, technology, or operational practices.

Privacy Notice

This Policy should be read in conjunction with Cobalt's General Privacy Notice, which outlines how we collect, use, and protect personal data across all services. The notice is available on our website or upon request.

Complaints and Escalation

Complaints or concerns regarding the use of CCTV or the handling of personal data should be directed to the Data Protection Coordinator at data protection@cobalthousing.org.uk. If a concern cannot be resolved internally, individuals have the right to escalate their complaint to the Information Commissioner's Office (ICO), the UK's independent authority for data protection.

Risk Management

The key risk associated with non-delivery of this Policy is:

Risk Register Ref:	Risk:
ST08	**Data and Records Management** Failure to manage the quality, integrity, security and governance of data resulting in regulatory and data management breaches, legal claims, fines and reputational damage.
Risk Consequences:	**Management and Mitigation:**
Breach of Regulatory Requirements Significant Financial Penalties with Data Protection Legislation of up to 4% of annual turnover per breach. Reputational Damage. There is also a risk of private claims/civil actions for breaches of Data Protection Legislation.	CCTV systems will be deployed in a manner that minimises intrusion and respects the privacy of individuals, including the use of privacy masking and strategic camera placement. Ensure correct installation and development of bespoke policy, guidance and procedures to underpin and ensure compliance to Surveillance Camera Code of Practice. Regular monitoring and quality testing of CCTV systems to check for vulnerabilities and access controls to system. Data Protection awareness and mandatory training including for any changes in legislation, internal changes or security concerns. Avoidance of excessive monitoring.

Regulatory & Legislative Compliance

- The Data Protection Act 2018
- Information Commissioners Office (ICO) requirements
- The UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998- UK Privacy Law
- Surveillance Camera Code of Practice

Links to Other Key Documents

POL 08	Data Protection Policy
POL 43	Cobalt Privacy policy
Procedure 167	Managing CCTV and telephone recording access requests
Procedure 001	Subject Access Requests
Procedure 002	Information security and breaches
QR 004	Request to View and or copy CCTV footage

Definitions

Data Controller – The entity that determines the purpose and means of processing personal data.

Data Subject – An identifiable individual whose personal data is collected, stored, or processed by an organisation.

CCTV Footage – Video recordings captured by surveillance cameras, stored digitally or on physical media for later review.

Subject Access Request (SAR) – A formal request by an individual to access personal data held about them by an organisation.

Privacy Masking – The digital obscuring (eg blurring or blocking) of parts of video footage – such as faces, license plates, or private property – to protect non-targeted individuals and comply with data protection laws.

Governance of this Policy

Equality Diversity & Inclusion (ED&I)	An EQIA has been completed on 24/10/25
Financial and Links to VfM	Effective management of personal data — including special category data captured via CCTV — is critical to safeguarding Cobalt's financial integrity and reputation. By ensuring compliance with data protection legislation and implementing robust controls around CCTV operations, Cobalt: • Minimises the risk of regulatory fines resulting from data breaches or unlawful processing • Reduces exposure to legal claims and reputational damage • Demonstrates a commitment to value for money (VfM**)** by investing in secure, compliant systems that protect individuals and organisational assets This policy supports Cobalt's broader VfM objectives by promoting responsible data stewardship and mitigating financial and operational risks.
Privacy and Data Protection	This Policy directly supports Cobalt's commitment to upholding the principles of data protection and privacy in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Prior to the installation and operation of any CCTV system, Cobalt has completed a Data Protection Impact Assessment (DPIA) to: • Identify and assess potential risks to individuals' rights and freedoms • Implement appropriate technical and organisational safeguards • Establish a clear and lawful basis for processing under Article 6 of UK GDPR The DPIA forms part of Cobalt's broader accountability framework and ensures that CCTV systems are deployed transparently, proportionately, and in a manner that respects individual privacy. DPIA Completed
Health and Safety	The primary purpose of installing CCTV systems across Cobalt premises is to enhance security, deter criminal activity, and support the safety of individuals and property. In circumstances where health and safety legislation applies, it may take precedence over data protection legislation — but only where it can be clearly demonstrated that: • The use of CCTV is necessary and proportionate to address a specific health or safety risk • A thorough assessment has been conducted to evaluate the impact on individual privacy • Appropriate safeguards have been implemented to minimise intrusion and ensure lawful processing Cobalt will ensure that any such use of CCTV is fully documented, justified, and aligned with both health and safety obligations and data protection principles.
Development and Consultation	Consultation with Cobalt's Tenant Consultative Panel was completed on 10th September 2025. Wider consultation was completed in October 2025 with Cobalt colleagues