Closed-Circuit Television (CCTV) POLICY

This policy applies to all academies within Bonitas Multi-Academy Trust

Date last reviewed	Summer 2025
Review period	Every 2 years
Date of next review	Summer 2027
Owner	CEO / Head of IT
Approved by	Board of Trustees
Date approved	July 2025
Associated documents/information	• BT Data Protection Policy • BT Data Retention Policy • BT Complaints Policy. • Subject Access Request Procedure

1. Introduction

This policy outlines the Bonitas Trust's use of Closed-Circuit Television (CCTV) systems across its schools and premises. CCTV is used to:

- Provide a safe and secure environment for pupils, staff, and visitors
- Protect school property from damage, theft, or loss
- Assist in prevention and detection of crime
- Assist in establishing the cause of accidents or resolving incidents or disputes to prevent re-occurrence.
- To assist in managing the school

1.1. CCTV is part of the Trust's wider approach to safeguarding and site security. It is included within each school's data processing records and maintained in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.2 Each school operates its own CCTV system under the guidance of this Trust-wide policy. The deployment, maintenance, and monitoring of systems are locally managed by school leadership, with oversight from the Trust and the Trust's Data Protection Officer (DPO).

2. Legal Framework and Compliance

2.1 This policy aligns with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Information Commissioner's Office (ICO) guidance
- Surveillance Camera Code of Practice
- 🔗 ICO guidance: https://ico.org.uk
- 🔗 Surveillance Camera Code of Practice: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

2.2 The Trust relies primarily on Article 6(1)(f) of the UK GDPR – legitimate interests – as the lawful basis for operating CCTV systems. This includes the Trust's interest in maintaining a safe and secure environment, protecting individuals and property, and assisting in the investigation of incidents.

In certain cases, the Trust may also rely on Article 6(1)(c) – legal obligation – where the use of CCTV supports compliance with statutory safeguarding duties, health and safety requirements, or other legal responsibilities.

CCTV usage is always assessed to ensure that it is necessary, proportionate, and balanced against the rights and freedoms of individuals.

All authorised personnel with access to CCTV images receive appropriate training and understand their responsibilities under the law.

3. Statement of Intent

3.1. The Trust and its schools are committed to using CCTV responsibly and transparently, maintaining public confidence in its operation. CCTV signage is clearly displayed in all areas where cameras are in use. Signs explain the purpose of CCTV and provide contact details.

3.2. While the system enhances security, it may not capture every incident.

4. System Overview

4.1. CCTV systems across Trust schools typically comprise fixed-position cameras used for internal and external monitoring. These systems do not normally include audio recording capabilities. Where audio recording is in place, its use must be clearly justified, proportionate, and subject to appropriate additional controls, in line with data protection principles.

The specific number, placement, and operational settings of cameras are determined by each school's leadership team, subject to this Trust-wide policy.

4.2. On a day-to-day basis, access to view live and/or recorded CCTV footage will be limited to staff members within the Trust / School who have been granted appropriate authorisation by the CEO / Headteacher (e.g., reception staff, site teams). Access will remain restricted to those individuals with a legitimate need and must not be shared further without authorisation.

4.3. The CEO / Headteacher will ensure there are regular checks to confirm the efficiency of the system and in particular that equipment is properly recording and cameras are functioning to provide clear, usable images.

5. Camera Placement

5.1. CCTV cameras are positioned to fulfil the specific purpose for which they were installed and are located in clearly visible, prominent positions to ensure transparency for staff, pupils, and visitors.

5.2. Cameras are positioned to capture relevant areas without intruding on individuals' reasonable expectations of privacy. Every reasonable effort is made to avoid monitoring areas outside of school premises or beyond the system's intended scope.

5.3. CCTV cameras are never installed in areas where individuals have a heightened expectation of privacy, such as toilet facilities or changing rooms.

5.4. Staff may have access to general information about camera locations.

5.5. Headteachers will maintain an internal record detailing specific elements for the use of cameras at their school including camera locations and system operators, and carry out regular reviews to ensure policy compliance.

6. Data Storage and Retention

6.1. Recorded CCTV images are typically retained for a maximum of 30 days, unless a specific incident requires longer retention, in which case justification will be documented.

6.2. Any retention of records for a period longer than this will need to be recorded alongside the specific purpose for which they are being kept (e.g. active investigation or legal process).

6.3. The Headteacher will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place must include:

- Restriction of access to specific user accounts.
- The CCTV system being encrypted/password protected.
- The ability to make copies must be restricted to specified members of staff

Recordings are stored securely with access restricted to authorised staff.

7. Subject Access Requests (SARs) and Disclosure of CCTV Footage

7.1. Any individual recorded by CCTV is a data subject under UK data protection legislation and has the right to request access to personal data relating to them, including CCTV footage. This type of request constitutes a Subject Access Request (SAR).

7.2. SARs must be submitted in writing to the Headteacher or the Trust / School's designated Data Protection Lead (DPL) and include sufficient information (e.g., date, time, location) to enable identification of the relevant footage relating to them.

7.3. The Trust will respond within one calendar month of receiving a valid request. Requests are free of charge unless deemed excessive or manifestly unfounded, in which case a fee may apply or the request may be refused.

7.4. Upon receiving a request, the staff member responsible for managing the CCTV system (or a nominated representative) will review the footage relevant to the time and location specified. If the footage only contains images of the requester, access may be granted to view or receive a copy of the footage. This will be strictly limited to scenes involving the individual only.

7.5. If the footage includes other identifiable individuals, the DPO must assess whether:

- It is reasonable and lawful to disclose the footage;
- The images can be edited to anonymise third parties;
- Consent from the other individuals can be obtained;
- Or whether disclosure should be withheld to protect the rights of others.

7.6. A record of all disclosures must be securely maintained and include:

- The date of the request;
- The review process and decision;
- The individuals granted access and when;
- Whether copies of the footage were shared, including format and recipient details.

7.7. Access to CCTV footage is strictly limited to those with a legitimate operational or safeguarding need. It may also be used in accordance with the Trust's disciplinary or grievance procedures, subject to standard confidentiality requirements.

7.8. Disclosure to third parties (e.g., Police, legal representatives, contractors) is only permitted where it is lawful, necessary, and proportionate. Such requests must be made in writing to the Headteacher or the Trust / School's DPL and be recorded in the school's data sharing log.

7.9. Access may be refused if fulfilling the request would compromise the rights of others or prejudice an investigation.

8. Disclosure of images to third-parties

8.1. Recorded CCTV images will only be disclosed to third parties (i.e., individuals other than the data subject) where permitted under UK data protection legislation and in accordance with the Trust's Data Protection Policy.

8.2. Still images may be extracted from footage by the Headteacher only where it is necessary to fulfil a legitimate purpose as outlined in Section 1, and in taking account of advice provided Trust's DPO, if required.

8.3. CCTV images may be disclosed to law enforcement agencies, including the police or prosecution services, where this is necessary in connection with their lawful duties and consistent with the system's stated purposes.

8.4. If a request is received from law enforcement:

- It must be referred to the School's DPL;
- The request must be reviewed in line with the Trust's Data Protection Policy and Subject Access Request Procedure;
- Sufficient detail must be obtained (e.g., what is being investigated, time, location, individuals of interest) to enable an informed decision;
- Third-party images must be considered and, where necessary, advice sought from the Trust's DPO.

8.5. If a court order is received for disclosure of CCTV images, it must be complied with. However, the order must be carefully reviewed to determine exactly what is required, and advice should be sought from the Trust's DPO if there is any uncertainty.

8.6. All disclosures to third parties, including law enforcement or court-directed disclosures, must be fully documented, recording:

- The date of request;
- The basis for disclosure;
- Any redaction or consideration of third-party rights;
- Who accessed or received the footage, and in what format.

9. Copying and Transfer of CCTV Footage

9.1. CCTV footage will only be copied or transferred to another medium (e.g., USB drive, DVD, or cloud storage) where it is necessary for:

- A Subject Access Request;

- Disclosure to authorised third parties (e.g., police, legal representatives);
- Internal investigations (e.g., safeguarding, disciplinary or grievance procedures);
- Legal or insurance purposes.

9.2. All copies of CCTV footage must be handled as confidential personal data and stored securely. The medium must be encrypted or password-protected where possible and access strictly limited to authorised individuals.

9.3. Copies must not be made unnecessarily or retained longer than needed. Once the purpose for copying has been fulfilled, the copied media must be securely destroyed or wiped in accordance with the Trust's Data Retention and Disposal Policy.

9.4. A record must be kept of all copied footage, including:

- The reason for copying;
- The date and time the copy was made;
- Who authorised the copy;
- The individual or organisation to whom the footage was provided (if applicable);
- How the copy was stored or transferred;
- When and how it was destroyed (if applicable).

9.5. Staff must not copy, download, or distribute CCTV footage for any purpose other than those expressly permitted under this policy.

10. Misuse of CCTV systems

10.1. The misuse of CCTV systems could constitute a criminal offence. Any member of staff who breaches this procedure may be subject to disciplinary action.

11. Complaints

11.1. Any concerns about the operation or use of CCTV should be raised in the first instance with the relevant Headteacher. If the concern is not resolved through this route, individuals may escalate the matter in accordance with the Trust Complaints Policy.

11.2. Where the concern relates to data protection, individuals may contact the Trust / School DPL. If the issue remains unresolved, individuals have the right to raise their concern with the Information Commissioner's Office (ICO):

12. Oversight

12.1. The Trust Board is responsible for overall policy compliance and oversight.

12.2. The Trust's DPO provides advice, maintains records of processing, and monitors adherence to data protection laws across all schools.

13. Review of Policy

This policy will be reviewed every two years, or sooner if required due to legal, technological, or operational changes.

Appendix A – School-Specific Camera Arrangements

Each school should maintain:

Site Plan with Camera Locations	A visual plan of the school site showing the location of all CCTV camer (internal and external). Helps support transparency, review of coverag and compliance.
2. Monitoring Responsibilities	A record of staff roles or individuals authorised to monitor, review, an access CCTV footage. This should include access levels and any delegat responsibilities.
3. System Specifications	Key technical information, including camera types (e.g., fixed, PTZ), resolution, whether audio is enabled, data storage method, retention settings, and system software version.
4. Local Operation Procedures	Any site-specific procedures that supplement or vary from the Trust-wide CCTV policy. Examples include incident escalation routes, review frequency, or designated safeguarding leads for CCTV.