# Policy and Procedure

## CCTV (Closed Circuit Television) Policy

**Reviewed and approved by:**

Finance, Resource & Audit Committee c/o BCWCAT Trust Board

**Approval Date:**

21st October 2025

**Review Date:**

21st October 2027

**Version:**

1

## 1. Introduction

The Blessed Christopher Wharton Catholic Academy Trust (BCWCAT) operates Closed Circuit Television (CCTV) systems across its academies to deter, prevent and detect crime; to safeguard pupils, staff and visitors; to protect Trust property; and to support the safe and effective operation of Trust sites.

This Policy sets out the principles, roles and responsibilities for the lawful, fair and proportionate operation of CCTV across BCWCAT. It must be read alongside the following Trust policies: Data Protection Policy (2025), Online Safety Policy (2025), Staff Acceptable Use Policy (AUP) (2025), Student Acceptable Use Agreements (2025), AI in Education Policy (2025), Freedom of Information Policy (2025), and the Privacy Notices for Visitors and for Pupils & Families.

CCTV systems may include conventional video cameras and AI-enabled analytics modules (e.g., Automatic Number Plate Recognition (ANPR), facial recognition, and object detection). Such features are subject to enhanced safeguards as set out in this Policy.

## 2. Scope and Policy Statement

- Applies to all BCWCAT academies and central Trust sites, and to all staff, contractors and authorised third parties who operate or access Trust CCTV systems.
- CCTV will be operated in compliance with UK GDPR, Data Protection Act 2018, the ICO CCTV guidance, the Online Safety framework and relevant safeguarding expectations.
- CCTV will not be used to monitor the performance of staff or pupils; it is used for site safety, safeguarding and security.
- Audio capture is disabled by default. Audio may only be enabled for specific, short-term safeguarding or safety purposes authorised by the Headteacher and DPO following a DPIA.

## 3. Lawful Basis and Data Protection Principles

The primary lawful basis for CCTV operation is the Trust's public task (UK GDPR Article 6(1)(e)). In emergencies, processing may rely on vital interests (Article 6(1)(d)). Where biometric data are processed for the purpose of uniquely identifying a person (e.g., facial recognition), the Trust will rely on an appropriate Article 9 condition and apply heightened safeguards. All CCTV processing adheres to data protection principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

## 4. Roles and Responsibilities

- Trust Board: approves this Policy; receives assurance on compliance and risk.
- Chief Executive Officer (CEO): ensures adequate resources and oversight for compliance and safe operation.
- Headteachers: accountable for local implementation and compliance at academy level; ensure signage, local procedures and staff briefings are in place.
- IT Director & Estates/IT Managers: system ownership and operation; secure configuration; access control; backups; maintenance; vendor management; training and audit.
- Designated Safeguarding Leads (DSLs): ensure CCTV use aligns with safeguarding processes and avoids placement in areas of high privacy (toilets, changing rooms).
- Data Protection Officer (DPO): advises on and monitors data protection compliance; approves DPIAs; manages subject access requests and data breaches; maintains the CCTV processing record (RoPA).
- Authorised Operators: only trained, authorised staff may access live view or recordings; must comply with this Policy and the Operator Code of Conduct (Appendix A).

## 5. Camera Siting and Installation

- Cameras will only be installed where necessary and proportionate to the stated purposes.
- No cameras in areas where there is a reasonable expectation of privacy (e.g., toilets, changing rooms, medical rooms).
- Use in classrooms is exceptional and must be justified by a DPIA and Headteacher/DPO approval, with clear time limits and safeguards.
- Before any new installation or significant change, a Data Protection Impact Assessment (DPIA) must be completed and approved by the DPO and Headteacher; consultation with affected groups will occur where appropriate.
- Each academy will maintain a local 'CCTV Asset Register & Camera Location Map' and a log of DPIAs for CCTV placements and analytics features.

## 6. AI-Enabled Features (ANPR, Facial Recognition, Object Detection)

- AI features will only be enabled where strictly necessary, proportionate and effective for clearly defined purposes (e.g., car-park security via ANPR, detection of weapons/objects posing immediate risk).
- Facial recognition (FR) or other biometric identification will not be used for routine attendance or conduct monitoring. Any use requires a DPIA, DPO approval, Headteacher sign-off, clear signage/transparency, and strict role-based access to any watchlists or matches.
- Automated decision-making about individuals is prohibited. Any alert generated by AI must be reviewed by authorised staff ('human-in-the-loop') before action is taken.

- Biometric templates and analytics metadata will be minimised, encrypted, access-controlled, and retained only for the shortest necessary period consistent with the purpose.
- Where FR is used for a specific safeguarding or security purpose (e.g., to identify a known offender subject to court orders), the legal basis, scope, retention, watchlist composition and review frequency must be documented in the DPIA and reviewed at least termly.

## 7. Mobile Application Use by Authorised Staff

- Authorised staff may install the approved CCTV mobile application to connect to the on-site server only where multi-factor authentication (MFA) or biometric device login is enforced.
- Mobile access must use encrypted connections and device security (screen lock, no sharing, auto-timeout).
- Staff must not use personal devices to download, store, screenshot, or share CCTV images or video of children or any data subjects. Exports must only be performed on Trust-managed devices to approved secure locations.
- Where technically supported, Trust mobile device management (MDM) will be used to enforce security policies for authorised devices; access will be removed immediately when no longer required.

## 8. Access Control, Viewing and Exports

- Access to live view and recordings is strictly limited to trained, authorised users under least-privilege principles; all access is logged and routinely audited.
- Exports will include a chain-of-custody record. Where feasible, third-party identities will be redacted or blurred before disclosure unless disclosure is to law enforcement.
- Unauthorised staff (i.e., those without system access) may submit a request to view or obtain CCTV footage via the DSL or Headteacher. Such a request will be considered, but **does not** create an entitlement to access; access will only be granted where the DSL/Headteacher (with DPO advice where needed) deems it lawful, proportionate, and appropriate.
- Internal viewing by staff will be supervised/recorded and proportionate to the stated purpose (e.g., investigating an incident).

## 9. Subject Access Requests (SARs) and Other Requests

- Individuals can request access to images of themselves under data protection law. Requests must be made in writing to the academy Headteacher or Trust Governance Team/DPO. Proof of identity will be required.
- Responses will be provided within one calendar month, subject to lawful exemptions and to the rights and freedoms of others. Where images of others are present, redaction may be required.

- Freedom of Information (FOI) requests for CCTV will be considered under FOI legislation; personal data will not be disclosed under FOI.
- Law enforcement requests will be handled promptly, with identity verified, legal basis recorded, and all disclosures logged.

## 10. Retention, Storage and Security

- Standard retention period for CCTV footage is 30 days, unless footage is required longer for an active investigation, legal proceedings or insurance claim. Retention periods for AI analytics metadata and biometric templates will be the minimum necessary and documented in the DPIA.
- All footage and metadata will be stored securely, encrypted at rest where supported, with role-based access controls, system hardening and regular security updates.
- Backups (where used) will be encrypted and access-controlled. Any export media will be uniquely labelled and stored securely with a chain-of-custody record.

## 11. Signage and Transparency

- Clear and visible signage will be displayed at site entry points and in monitored areas, stating that CCTV is in operation, the purposes (security/safeguarding/crime prevention), and contact details for the academy and the Trust DPO.
- Privacy information about CCTV will be included in the Trust and academy privacy notices and websites. Where AI analytics (e.g., ANPR/FR/object detection) are enabled, transparency statements will be updated and displayed where appropriate.

## 12. Vendor and Third-Party Management

- The Trust will use suppliers who can demonstrate compliance with UK data protection law and good security practice; appropriate data processing agreements will be in place.
- Data will not be transferred outside the UK (or UK-adequate countries) without appropriate safeguards.
- Third-party engineers will only access systems under supervision, with access logged and time-limited.

## 13. Maintenance, Testing and Audit

- Systems will be maintained regularly to ensure reliable recording and evidential quality.
- Annual audits will confirm: up-to-date ICO registration; responsible persons; signage accuracy; coverage justification; access logging; retention enforcement; operator training; and effectiveness.
- DPIAs and any AI-enabled features will be reviewed at least annually and sooner if the risk profile changes.

## 14. Covert Monitoring

- Covert monitoring is only permitted in exceptional circumstances (e.g., serious crime or gross misconduct) where notification would prejudice the investigation.
- Covert deployments require CEO/Headteacher authorisation and DPO advice, must be time-limited and proportionate, and are never permitted in private areas.

## 15. Incident Response and Data Breach Management

- Suspected or actual personal data breaches involving CCTV (e.g., unauthorised disclosure or loss of footage) must be reported immediately to the DPO and handled under the Trust's Data Breach Procedure.
- Where appropriate, the ICO and affected individuals will be notified in accordance with legal obligations.

## 16. Training and Awareness

- Authorised operators will receive training on lawful use, system operation, exports, redaction, and this Policy.
- Induction and annual refreshers will remind staff of prohibited behaviours (e.g., downloading footage to personal devices, sharing images on social media).

## 17. Governance, Review and Version Control

This Policy is owned by the IT Director and reviewed by the DPO. It will be reviewed every two years or earlier if there is a material change to law, guidance, technology or risk. Local appendices (camera location maps, signage examples, DPIA register) are maintained by each academy.

## Appendix A – CCTV Operator Code of Conduct

- Only operate CCTV if you are authorised and trained.
- Keep all information confidential; do not discuss footage outside authorised channels.
- Do not download or copy footage except where authorised; never use personal devices.
- Log all access, viewing and exports; follow chain-of-custody procedures.

## Appendix B – Subject Access Request (CCTV) Guidance

1. Make a written request to the academy Headteacher or Trust Governance Team/DPO and provide proof of identity.
2. Specify date/time/location to help us identify relevant images. We cannot release images of other people without their consent unless it is reasonable and lawful (redaction may be applied).

3. We will respond within one calendar month and explain any lawful limitations or redactions required to protect others' rights.

## Appendix C – Annual CCTV Audit Checklist (per Academy)

- ICO registration up to date; purpose recorded.
- Named responsible officers (Headteacher, Estates/IT lead, DPO).
- Signage accurate and visible at entry points and monitored zones.
- Camera coverage justified and proportionate; no cameras in private areas.
- DPIAs completed/updated for installations and AI features (ANPR/FR/object detection).
- Retention period enforced; deletion processes tested.
- Access controls, MFA/biometrics on mobile app; access logs reviewed.
- Export procedures and chain-of-custody in place; redaction capability available.
- Operator training records current; staff awareness refreshed annually.
- Maintenance/testing performed and recorded; image quality sufficient for evidential purposes.

Policy Owner: IT Director | Contact: governance@bcwcat.co.uk | DPO: dpo@bywaterkent.co.uk