CCTV and Surveillance Policy

Version:	v1.0
Policy Type:	Operations – Statutory
Approval date:	16 March 2028
Approved by:	Trust Board
Next review:	Spring 2029

Together we Exceed

Contents

1. Policy Statement

1.1 Exceed Academies Trust uses CCTV and other video surveillance systems to promote the safety and welfare of pupils, staff, visitors and contractors; to protect school property; to deter and detect crime; and to support the effective management of incidents.

1.2 The purpose of this policy is to set out the Trust's approach to the lawful, safe and proportionate use of CCTV and surveillance systems and ensure that:
- We comply with the UK GDPR and Data Protection Act 2018
- The images captured are useable for legitimate purposes
- Individuals are reassured that their images are handled in accordance with data protection legislation

1.3 CCTV is deployed only where it is necessary and proportionate to achieve legitimate aims. The Trust does not use CCTV for routine staff monitoring.

1.4 This policy relates to the location, operation, recording, storage and use of video surveillance systems. The Trust complies with the Information Commissioner's Office (ICO) Video Surveillance Guidance.

1.5 The video surveillance systems are included in Exceed Academies Trust's registration with the ICO as a Data Controller.

1.6 Systems are owned and operated by Trust schools or third-party providers. Where a third party operates the system, a compliant Data Processing Agreement must be in place and associated risks managed through a Data Protection Impact Assessment (DPIA).

1.7 CCTV equipment records visual images only. Audio recording is disabled across the Trust. Any proposal to introduce audio capability must be supported by a DPIA and approved by the Data Protection Officer (DPO).

1.8 Drones may be used only for estates-related functions (e.g. roof inspections) or approved educational purposes. Drone use must:
- Be pre-approved by the Head of Estates and DPO
- Be supported by a DPIA
- Comply with Civil Aviation Authority (CAA) regulations, including operator competency and registration
- Avoid capturing neighbouring properties, the public highway, or areas outside the school boundary unless strictly necessary and legally justified
- Ensure any captured imagery is treated as personal data where identifiable individuals could be seen

1.9 This policy must be read in conjunction with:
- Photography and Images Policy
- Online Safety Policy
- Freedom of Information Policy
- School Security Policy
- Data Protection Policy & DPIA procedures
- Records Management Policy
- Whistleblowing Policy (for concerns regarding CCTV misuse)

1.10 This policy has due regard to relevant legislation and guidance including:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- Data (Use and Access) Act 2025
- Protection of Freedoms Act 2012
- Surveillance Camera Code of Practice (2021)
- Freedom of Information Act 2000
- Human Rights Act 1998
- Equality Act 2010
- ICO CCTV and Video Surveillance Guidance

2. Definitions

2.1 For the purpose of this policy the following definitions are given for the below terms:

- CCTV / Surveillance systems: Fixed or mobile systems capturing visual images for surveillance.
- Overt surveillance: Surveillance that is clearly visible and signposted.
- Covert surveillance: Conducted without individuals' knowledge. The Trust does not undertake covert surveillance under any circumstances. Any covert activity on Trust premises must be initiated, authorised and directed solely by law enforcement.
- Personal data: Information about an identifiable individual.

Note: The Trust prohibits staff-initiated covert recording for any purpose.

3. Roles and responsibilities

3.1 **Trust Board**

- The Trust is the Data Controller for all CCTV systems across its schools.
- Trustees ensure governance, compliance and appropriate resourcing.

3.2 **Data Protection Officer (DPO)**

- Provides expert advice on DPIAs and lawful processing.
- Oversees SARs and FOI requests in relation to CCTV.
- Maintains records of processing activities.
- Monitors compliance and reports concerns to senior leadership.

3.3 **Headteachers**

Headteachers act as operational leads on behalf of the Data Controller. They must:

- Decide CCTV deployment in consultation with the DPO and Chief Estates Officer.
- Ensure signage is in place.
- Ensure staff understand their responsibilities.
- Approve access requests for footage.
- Conduct annual CCTV reviews (with Estates and the DPO).

3.4 **Chief Estates Officer**

- Ensures installation, maintenance and technical security of systems.
- Conducts annual camera placement effectiveness reviews.

3.5 **ICT Technical Lead & Site Managers (Data Processors)**
- Ensure technical security controls, robust authentication and system resilience.
- Manage data extraction, secure transfer and deletion following authorisation.

4. Purpose and Justification

4.1 CCTV may be used for:
- Safety and welfare of pupils, staff and visitors;
- Protection of premises and assets;
- Crime prevention and detection;
- Incident and behaviour management;
- Supporting investigations by the Trust or authorised agencies.

4.2 All deployments of CCTV must be supported by a DPIA demonstrating: necessity, proportionality, consideration of less intrusive alternatives, and mitigation of risks.

5. Data Protection and DPIAs

5.1 All CCTV processing complies with UK GDPR principles.

5.2 A Data Protection Impact Assessment must be completed and approved by the for:
- New installations
- Significant changes
- Audio enablement proposals
- Drone usage on school sites

5.3 If a DPIA identifies unmitigated high risks, the Trust will consult the ICO before proceeding.

5.4 Procurement of CCTV systems must include:
- Supplier due diligence
- UK data hosting and security assurances
- Contracts including GDPR-compliant Data Processing Clauses

6. Operation of CCTV Systems

6.1 Access to CCTV systems is restricted to authorised staff only and protected by strong authentication.

6.2 Clear and prominent signage must be displayed at all CCTV locations.

6.3 Cameras must not be directed at private areas.

6.4 CCTV must not target individuals or groups unless responding to a live incident.

6.5 Camera placement must be reviewed annually by the Headteacher and Chief Estates Officer, with oversight from the DPO.

6.6 System faults must be addressed promptly.

6.7 Cyber-security standards apply, including:
- Multifactor authentication where available
- Encrypted storage and encrypted export of footage
- No cloud storage unless DPO-approved and UK-hosted

7. Security and Retention

7.1 All recordings are securely stored and protected from unauthorised access.

7.2 Authorised operators:
- Headteacher
- DPO
- Chief Estates Officer
- ICT Technical Lead
- Site Manager (data processor).

7.3 Routine CCTV footage is retained for 30 days (or less where a system dictates) unless required longer for an active investigation, safeguarding concern, disciplinary matter, insurance claim or legal process. Extended retention requires:
- A justification recorded in the CCTV retention log
- Review every 30 days

7.4 Footage no longer required must be securely and irreversibly deleted.

7.5 Unauthorised access or misuse may result in disciplinary action and potential criminal investigation.

7.6 Concerns about CCTV misuse may be raised via the Trust's Whistleblowing Policy.

8. Covert Surveillance

8.1 The Trust does not undertake covert surveillance.

8.2 If law enforcement agencies require covert surveillance on Trust premises, this will only occur under their lawful authority and direction. The Trust will cooperate with such agencies as required but will not initiate, authorise, or manage covert surveillance activity.

9. Access to CCTV Footage

9.1 Individuals may request access to CCTV footage in which they appear via a Subject Access Request (SAR).

9.2 All CCTV recordings remain the property of the Trust. Access will be granted only where it is lawful, safe, and appropriate to do so.

9.3 Where footage contains third parties, their identities will be protected through redaction or by supervised viewing if redaction is not feasible.

9.4 The Headteacher, in consultation with the DPO, will decide whether footage, still images, or a supervised viewing is the most appropriate method of access in each case.

9.5 The school may refuse a request where disclosure would:
- unreasonably reveal third-party personal data that cannot be redacted
- prejudice a police or safeguarding investigation
- compromise the security or operation of the CCTV system
- fall within a lawful exemption

9.6 Disclosures to authorised third parties (e.g., police, insurers, legal representatives) will only be made where lawful, necessary and proportionate.

9.7 Requests for CCTV under the Freedom of Information Act will be processed under FOI procedures; however, CCTV footage is normally exempt where it contains personal data.

9.8 The Trust's Data Protection Policy and Subject Access Request Policy set out the full SAR process, timescales, ID verification requirements, and rights of individuals. This CCTV and Surveillance Policy should be read alongside those policies.

10. Monitoring and Review

10.1 This policy will be reviewed every three years, or sooner if required by legislative or operational changes.

10.2 The DPO will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

10.3 Headteachers are responsible for communicating updates to their staff.

Appendix 1 - CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE

1 Who will be captured on CCTV?

Pupils, staff, parents / carers, volunteers, Governors and other visitors including members of the public etc.

2 What personal data will be processed?

Visual images only (audio is disabled Trust-wide unless specifically authorised by a DPIA and DPO approval)

3 What are the purposes for operating the CCTV system? Set out the problem that the Trust is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

Prevention or detection of crime and reduce anti-social behaviour around sites, manage workforce issues including use within disciplinary procedures

4 What is the lawful basis for operating the CCTV system?

Legal Obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime

5 Who is/are the named person(s) responsible for the operation of the system?

Estates Team School Site Teams Headteachers / Principal of each school

6 Describe the CCTV system, including:

a. Each school site has a fixed CCTV system with cameras located within the school grounds (internally and externally). The cameras are high specification to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained.

b. Cameras have been sited within the School grounds to avoid capturing images which are not necessary for the purposes of the CCTV system;

c. Signs indicating that CCTV is in operation are located at various locations within the site. These are located on the main entrances, within the car park and footpaths throughout school so that they are clearly visible to all stakeholders.

7 Set out the details of any sharing with third parties, including processors

CCTV footage maybe provided to external parties such as the Police, or through subject access requests. Careful consideration will be given to whether any provider is used in relation to the CCTV system and the access they might have to images.

The CCTV system is monitored by a third party monitoring company who have direct access to live images of the CCTV system once the system is armed on the schedule. All recording data is stored on the CCTV system itself, on individual hard drives located inside the unit.

8 Set out the retention period of any recordings, including why those periods have been chosen

30 days retention

9 Set out the security measures in place to ensure that recordings are captured and stored securely

Access restricted to authorised individuals.
Encrypted storage and export processes.
The footage is stored on the CCTV Server with no other access

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

- Identification of an individual
- Loss of data if recordings disclosed to a third party (such as the police) if data not encrypted
- Misuse of data if accessed by non-authorised individual

11 What measures are in place to address the risks identified?

- Is it fair to record them in the way proposed? Yes, we have a duty of care to our pupils, staff and visitors and CCTV facilitates this
- How is the amount of data processed to be minimised? 30 days retention period and only accessed by key individuals
- What are the risks of the system being accessed unlawfully? Low – password protected and only key individuals have access
- What are the potential data breach risks? CCTV footage released publically without consent – loss of data.

• What are the risks during any transfer of recordings, or when disclosed to third parties such as the police? Loss of data – Secure Encrypted USB to be used when transferring any data

12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

CCTV Installation was approved by the LGB of each school (each school having parent governors).

13 When will this privacy impact assessment be reviewed?

As required or with any changes to CCTV system in any of the schools.

Approval:

This assessment was approved by the Data Protection Officer:

DPO ……Ruth Jarvis ……
Date ……March 2023…….