



Mowbray Education Trust

CCTV Policy

June 2026

Document Type	Published online and available to all staff
Last Revision Date	June 2026
Next Revision Date	June 2028 (or sooner if statutory guidance changes)
Owner	Trust IT Lead
Author	Trust IT Lead
Version	1.0
Status	Approved by AFR June 2026

This policy applies to.....	3
1. Introduction and Objectives.....	3
2. Relevant legislation and guidance	3
3. Privacy and Data Protection Impact Assessments (DPIAs).....	4
4. Camera Positioning and Warning Signs.....	4
5. Data Retention	4
6. Access and System Security.....	4
7. Disclosure to Third Parties.....	5
8. Subject Access Requests (SARs).....	6
9. Complaints and Breaches	6
Log of Changes to Document.....	7

This policy applies to:

All Trust settings.

Where this policy states 'school' this means any of our educational establishments and the wider Trust.

Where this policy states 'Headteacher' this also includes 'Head of School' and 'Centre Manager.'

Mowbray Education Trust (MET).

1. Introduction and Objectives

This policy regulates the management, operation, and use of closed-circuit television (CCTV) systems across the Trust, ensuring compliance with the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR). The primary objectives of the CCTV system are to:

- Safeguard students, staff, and visitors, and reduce the fear of crime.
- Protect school buildings and assets from damage or theft.
- Support the police in deterring and detecting crime, and assist in identifying and prosecuting offenders.
- Assist in establishing the cause of accidents and managing the school effectively, including resolving disciplinary disputes.

Breaches of this policy will be dealt with under the Mowbray Education Trust Conduct and Disciplinary Policy and in some cases criminal proceedings.

2. Relevant Policies & Legislation

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- ICT Acceptable Use Policy
- Keeping Children Safe in Education (KCSIE)
- Conduct and Disciplinary Policy

3. Privacy and Data Protection Impact Assessments (DPIAs)

The Trust recognises that CCTV systems can be privacy-intrusive. To evaluate whether the CCTV system is a necessary and proportionate means of achieving our legitimate objectives, the Trust utilises Data Protection Impact Assessments (DPIAs).

- A DPIA will be carried out when installing new systems, replacing, or upgrading existing cameras.
- Cameras will generally not be placed in areas where individuals have a heightened expectation of privacy. If a legitimate need arises to place cameras in sensitive areas (e.g., toilets or changing facilities), a DPIA will be conducted and stakeholders will be consulted prior to installation.
- If covert surveillance or audio recording is ever deemed strictly necessary for extreme circumstances (e.g., suspected criminal offences), a DPIA will be completed to ensure compliance with data protection law.

4. Camera Positioning and Warning Signs

- **Positioning:** Cameras are positioned to maximise effectiveness but must not be directed to track individuals or focus on adjacent private homes, gardens, or off-site private property.
- **Signage:** Prominent warning signs are clearly displayed at strategic points and building entrances to inform staff, students, and visitors that CCTV is in operation.

5. Data Retention

CCTV footage is not retained longer than necessary. Recordings are held on the system memory for a standard period of **30 days**, after which they are automatically overwritten or deleted. The only exception is if images are required for ongoing legal reasons, such as an active police investigation, in which case they will be securely retained for a longer specified period.

6. Access and System Security

To protect the integrity of the system and ensure the privacy of all individuals, the management and access of CCTV is governed by stringent security protocols. The following measures are designed to safeguard recorded footage against unauthorised access, tampering, or misuse:

- **Restricted Access:** Access to the CCTV system, control rooms, and recorded data is strictly restricted to named authorised personnel only—Headteacher, Designated Safeguard Leads (DSLs & DDSLs), Data Protection Officer (DPO), System/Network Manager, and specific facilities staff.
- **Access as a Last Resort:** The system will only be accessed as a last resort, after all other reasonable lines of inquiry or alternative eventualities have been fully exhausted.
- **Viewing Stations:** Dedicated CCTV viewing monitors must be located exclusively within the offices of the Headteacher, Senior Leadership Team (SLT), Designated Safeguard Leads (DSLs) or pre-agreed locations. This placement ensures that any live or recorded playback is fully monitored, shielded from unauthorised eyes, and accessible only under direct, approved supervision.
- **Security Measures:** The system and data are protected by passwords, encrypted wherever possible, and kept in secure areas.
- **Access Logs:** Whenever footage is viewed, accessed, or downloaded, a detailed electronic record must be maintained. This log must include the time, date, name of the person accessing the footage, and the purpose of the access.
- **Media Handling:** If footage must be downloaded for evidential purposes, the media must be encrypted, sealed, witnessed, signed by the controller, and kept in a secure store.
- **Prohibition of Reproductions:** The unauthorised copying or reproduction of CCTV footage by any secondary means - including, but not limited to, screenshots, recording with mobile phones, or utilising any other digital devices - is strictly prohibited. All official data exports must follow designated evidential download protocols.

7. Disclosure to Third Parties

- Materials secured via CCTV will never be used for commercial purposes or media entertainment.
- Images may be viewed by or released to the police or other authorised agencies strictly for the prevention and detection of crime, after all school data protection

reporting procedures have been followed. Any media handed over remains the property of the Trust.

8. Subject Access Requests (SARs)

Under GDPR, individuals (data subjects) have the right to request access to personal information, including CCTV images of themselves.

- Requests must be made in writing and should include sufficient details (date, time, location) to help locate the footage.
- The Trust will respond promptly, within 30 days or one calendar month of receiving the request.
- To protect the privacy of others, images of third parties captured in the request may result in footage being limited down to a smaller time frame, still images only, or the request denied after all reasonable attempts have been made.

9. Complaints and Breaches

Any complaints regarding the operation of the CCTV system should be addressed to the Headteacher and handled in line with the School's formal Grievance or Complaints Procedures.

Breaches of this policy will be dealt with under the Mowbray Education Trust Conduct and Disciplinary Policy and in some cases criminal proceedings.

Log of Changes to Document

Version	Date	Page	Change	Approver
V1.0	Jun 26	All Pages	New policy created for MET Executives review and approval	MET Executives