



CCTV Policy

2026 -2027

Compiled/ Reviewed and Updated	Author: Dave Hutchinson	Date: April 2026
Approval By: CEO/ Executive Team – P Montalto	Approval Date: 30 April 2026	Review Date: April 2027

Contents

1. CCTV	3
2. Objectives	3
3. Purpose of the policy	3
4. Statement of intent	3
5. System management	4
6. Downloading captured data on to other media	5
7. Complaints about the use of CCTV	7
8. Requests for access by the Data Subject	7
9. Public information	7

1. CCTV

The Trust recognises that CCTV systems can be privacy intrusive.

The term 'Trust' includes all schools and organisations within DMAT

2. Objectives

Review of this policy shall be repeated regularly and whenever new technology is introduced, a review will be conducted, and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist the Trust in reaching the following objectives:

- (a) Pupil behaviour, access control, staff conduct investigations, 5 bells/lockdown, lettings -monitoring of activities etc
- (b) To increase a sense of personal safety and reduce the fear of crime
- (c) To protect the Trust buildings and assets
- (d) To support the police in preventing and detecting crime
- (e) To assist in identifying, apprehending, and prosecuting offenders
- (f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence

3. Purpose of the policy

Transparency, signage, and privacy information

Prominent signage is displayed at site entrances and monitored zones stating that CCTV is in operation, the purposes, and the controller's contact details and DPO contact. The Trust's privacy notice includes details of CCTV processing, retention, sharing, and how to exercise information rights. Audio recording is enabled in some cameras and only used in exceptional, clearly justified circumstances with additional signage.

The purpose of this policy is to regulate the management, operation, and use of the CCTV system (closed circuit television) in the Trust. The CCTV systems owned and operated in DMAT schools each comprise of both fixed and dome cameras (the number and coverage being dependent on the size and need of the site/school). The cameras within each system are strategically located to best meet the needs of the local site/school context. Locations are regularly reviewed to ensure they remain fit for purpose. Signage will be placed on/around all site entrances to highlight to visitors that CCTV is in use.

CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

4. Statement of intent

Surveillance Camera Code of Practice

The Trust takes account of the Home Office Surveillance Camera Code of Practice (2021) and its 12 guiding principles, reviewing camera placement annually to ensure use remains lawful, necessary, and proportionate.

Lawful basis and DPIA

The Trust operates CCTV under Articles 5 and 6 UK GDPR and the Data Protection Act 2018 for specified, explicit and legitimate purposes (e.g., safety, crime prevention, and protection of assets). For schools and academies acting as public authorities this is under the lawful basis of public task; where appropriate, legitimate interests may apply subject to a documented Legitimate Interests Assessment (LIA). Prior to installation or material change, a Data Protection Impact Assessment (DPIA) is completed to assess necessity and proportionality, risks to individuals (including children) and mitigations.

CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are displayed where relevant so that staff, students, visitors, and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

The CCTV system will seek to comply with the requirements both Data Protection Act and the most recent Commissioner's Code of Practice.

The Trust will treat the system, all information, documents, and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed as far as possible to deny observation on adjacent private homes, gardens, and other areas of private property.

Materials or knowledge secured because of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, will be clearly visible on the site and make clear who is responsible for the equipment.

CCTV images are not retained for longer than necessary, considering the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of typically 14 to 30 days (unless a shorter or longer period is justified by purpose).

Recorded images will only be retained long enough for any incident to become known (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than necessary and subject to documented justification (default maximum: 6 months where an incident requires retention).

5. System management

Third-party processors and DUAA obligations

All vendors or service providers with access to CCTV systems or footage must sign a Data Use and Access Agreement (DUAA) or equivalent data processing terms. The DUAA requires: processing only on documented instructions; role-based access; security controls (encryption/MFA); breach notification without undue delay to enable ICO notification within 72 hours where required; restrictions on onward disclosure; sub-processor approval; support with SARs; secure return/deletion on termination; and Trust audit rights.

Biometric identification, facial recognition, and automated analytics

The Trust does not deploy facial recognition or other biometric identification via CCTV. Any proposal to do so would require a specific lawful basis, an Article 9 condition, explicit transparency measures suitable for children, and a DPIA approved by the DPO and Trust leadership before any deployment. Any automated analytics will not be used to make decisions about individuals without meaningful human involvement.

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be managed by Data Protection Officer who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by Chief Operating Officer.

The system and the data collected will only be available to the authorisation list of each school

The CCTV system is designed to be in operation 24 hours a day and 7 days a week, though the Trust does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and that the equipment is properly recording and that the cameras are functional.

Cameras have been selected and positioned to best achieve the objectives set out in this policy by providing clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property, or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above requests access to the CCTV data or system, the System Manager must satisfy themselves of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

All visitors sign in at school receptions, and these records are kept for the length of retention period of CCTV recordings of each school.

6. Downloading captured data on to other media

Incident response and breach reporting

Any personal data breach involving CCTV will be escalated immediately to the DPO in line with the Trust's Data Breach Policy. Notifiable breaches will be reported to the ICO without undue delay and, where feasible, within 72 hours of awareness.

To maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- (a) Each downloaded media must be identified by a unique mark.
- (b) Before use, each downloaded media must be cleaned of any previous recording.
- (c) The System Manager will register the date and time of downloaded media insertion, including its reference.
- (d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made later providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
- (e) If downloaded media is archived, the reference must be noted.
- (f) If downloaded media is put onto a device, the device will be encrypted, and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, their replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the Trust and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the Trust to retain the downloaded media for use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the Trust's Data Protection Officer and a decision made by a senior leader of the Trust/ school in consultation with the Trust's Data Protection Officer.

School investigations

CCTV footage may be used to support investigations into alleged staff misconduct, breaches of Trust policies, safeguarding concerns, or other behaviour that may pose a risk to pupils, staff, visitors, property, or the effective running of the academy. Any access to, viewing of, or sharing of CCTV images for this purpose will be authorised in advance by the Headteacher (or nominated senior leader) and, where appropriate, in consultation with HR and/or the Data Protection Officer, ensuring the use is lawful, necessary, and proportionate.

CCTV will not be used for routine performance management or as a tool for general staff monitoring; it will only be reviewed where there is a clear, specific concern or reported incident and where other reasonable steps have been considered. Footage will be limited to relevant times and locations, handled confidentially, stored and retained in line with the MAT's retention arrangements, and shared only with those who have a legitimate need to know (for example, investigating officers, HR, the DPO, or the police). Where the footage is relied upon as evidence, it will be managed in a way that preserves its integrity and supports a fair process for all parties involved.

7. Complaints about the use of CCTV

Data subject rights and CCTV SARs

Individuals have the right to request access to footage that identifies them. Requests will be acknowledged and fulfilled within one month where feasible. The Trust will use appropriate redaction (e.g., blurring) to protect third parties or seek consent where appropriate. Disclosures are logged and made securely.

Any complaints in relation to the Trust's CCTV system should be addressed to:

DPO@dmateducation

8. Requests for access by the Data Subject

UK GDPR and the Data Protection Act 2018 provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to DPO@dmateducation

9. Public information

Copies of this policy will be available to the public from the Trust/ school offices.