

CCTV & Surveillance Policy

Summary

This policy document is to enable staff of Eastern Multi-Academy Trust to comply with legislation relating to CCTV in all circumstances.



If you are unsure about the validity of the content of this policy please refer to the Policy Owner.

Please Note: This policy is applicable to All Employees / Teachers / Support Staff / Volunteers including Trustees and Governors within the Group.

Policy owner	Audit Committee
Policy holder	Chief Executive Officer
Author	David Cousins, Chief Finance Officer Rebecca Schrooder, Operations Manager

Policy Inventory ID Number	DP06
Group Policy Area	IT Security and GDPR Policies

Approved by

Consultation Group	Audit Committee
Approval Committee	Audit Committee
Implementation date	July 2025
Review Date	July 2028

Version Control

Control No	Change summary	Consultation Group	Effective date
01	Addition of section 6 – covert recording	Audit	June 2025

POLICY AIM

This document will enable staff of Eastern Multi-Academy Trust to comply with legislation relating to CCTV in all circumstances.

1. EXECUTIVE SUMMARY

- 1.1 The purpose of CCTV is to protect staff, students and the public, discourage aggressive and abusive behaviour protect the Eastern Multi-Academy Trust infrastructure, and provide evidence where required to investigate complaints.
- 1.2 The policy will set out the purpose of using CCTV, what information will be recorded, who will have access to this information and how this information will be stored and disposed of.

2. POLICY STATEMENT

- 2.1. This Policy seeks to ensure that the Close Circuit Television (CCTV) system used at any Academy within Eastern Multi-Academy Trust is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (“DPA 2018”) and as amended from time to time) and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with privacy law. It considers best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. Eastern Multi-Academy Trust therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 2.2, and only if it is proportionate to that aim.
- 2.2. Eastern Multi-Academy Trust seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property, and premises.

Eastern Multi-Academy Trust therefore deploys CCTV to:

- promote a safe Eastern Multi-Academy Trust community and to monitor the safety and security of its premises, staff, and students.
 - assist in the prevention, investigation, and detection of crime.
 - assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
 - assist in the investigation of breaches of its codes of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.
- 2.3 This policy will be reviewed every three years by the EMAT Board, delegated to Audit Committee, to assess compliance with clauses 2.1 and 2.2 and to determine whether the use of the CCTV system remains justified.
 - 2.4 The operational requirements for the CCTV system in use across the Trust are documented in a “CCTV Operational Requirement Report”, held, and maintained by the Principal or Operations Manager at each Academy.

3. SCOPE

- 3.1 This policy applies to CCTV systems in all parts of Eastern Multi-Academy Trust and other related facilities.
- 3.2 This policy does not apply to any Webcam systems located in meeting rooms, classrooms or lecture theatres operated by Faculties, Departments or ICT, which are used for the purposes of monitoring room usage and to assist with the use of the audio-visual equipment.
- 3.3 This policy applies to all Eastern Multi-Academy Trust staff, contractors and agents who operate, or supervise the operation of, the CCTV system including Security Management and Staff and the Data Protection Officer.

4. ROLES AND RESPONSIBILITIES

- 4.1 The Trust Operations Team has the overall responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.
- 4.2 The Trust Operations Team is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 2.1 of this policy. Where new surveillance systems are proposed, the Trust Operations Team will consult with the Data Protection Officer to determine whether a data protection impact assessment is required.
- 4.3 Only the staff of EMAT IT Dept or Trust Appointed external IT contractor or a properly appointed maintenance contractor for Eastern Multi-Academy Trust's CCTV systems is authorised to install and/or maintain it.
- 4.4 The Trust Operations Team is responsible for the evaluation of locations where live and historical CCTV images are available for viewing. The list of such locations and the list of persons authorised to view CCTV images is maintained by the Trust Operations Team.
- 4.5 Changes in the use of Eastern Multi-Academy Trust's CCTV systems can be implemented only in consultation with Eastern Multi-Academy Trust Data Protection Officer or Eastern Multi-Academy Trust Legal Advisors.

5. SYSTEM DESCRIPTION – FIXED CAMERAS

- 5.1 The CCTV systems installed in and around Eastern Multi-Academy Trust's estate cover building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas. They continuously record activities in these areas and some of the cameras are set to motion detection.
- 5.2 CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

- 5.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently 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).*
- 5.4 The contact point for queries about CCTV around Eastern Multi-Academy Trust's estate should be available to staff, students, and members of the public during normal business hours. Any employees staffing the contact point must be familiar with this document and the procedures to be followed if an access request is received from a Data Subject or a third party.

6. COVERT RECORDING

- 6.1 Covert recording (i.e. recording which takes place without the individual's knowledge):
- 6.1.1 may only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e. there is no other reasonable, less intrusive means of achieving those purposes;
- 6.1.2 may not be undertaken without the prior written authorisation of the Chief Executive Officer. All decisions to engage in covert recording will be documented, including the reasons.
- 6.1.3 will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted; and
- 6.1.4 will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

7. OPERATING STANDARD

- 7.1 The operation of the CCTV system will be conducted in accordance with this policy.
- 7.2 Control room
- 7.2.1 No unauthorised access to the Security Control Room ("the Control Room") will be permitted at any time.
- 7.2.2 Access to the Control Room will be limited to:
- persons specifically authorised by the Principal or Trust SLT
 - Academy Leadership Team (Principals, Vice or Assistant Principals, Operations Managers)
 - EMAT Network & IT Manager
 - maintenance engineers.
 - police officers where appropriate; and
 - any other person with statutory powers of entry.
- 7.2.3 Monitors are not visible from outside the Control Room.
- 7.2.4 Before permitting access to the Control Room, managing staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors

are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the Control Room.

7.2.5 A log of shall be retained setting out the following:

- person reviewing recorded footage.
- time, date, and location of footage being reviewed; and
- purpose of reviewing the recordings.

7.3 Processing of Recorded Images

7.3.1 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstations, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

7.4 Quality of Recorded Images

7.4.1 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to clause 1 of these procedures are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained.
- cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.
- consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

8. RETENTION AND DISPOSAL

8.1 CCTV images are not to be retained for longer than necessary, considering the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce a maximum 60-day rotation in data retention.

8.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

8.3 All retained CCTV images will be stored securely.

9. DATA SUBJECT RIGHTS

- 9.1 Recorded images, which directly or in combination with other factors enable a data subject to be identified, are considered to be the personal data of the individuals whose images have been recorded by the CCTV system.
- 9.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.
- 9.3 Data Subjects can exercise their rights by submitting a request in accordance with Eastern Multi-Academy Trust policies.
- 9.4 On receipt of the request, the Data Protection Officer, or their representative, will liaise with the Trust Operations Team regarding compliance with the request, and subject to clause 8.5, the Data Protection Officer will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.
- 9.5 The period for responding to the request may be extended by two further months where necessary, considering the complexity and number of the requests. The Data Protection Officer will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

10. THIRD PARTY ACCESS

- 10.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:
- legal representative of the Data Subject.
 - law enforcement agencies including the Police.
 - disclosure required by law or made in connection with legal proceedings; and
 - HR staff responsible for employees and Academy staff responsible for students in disciplinary and complaints investigations and related proceedings.
- 10.2 Legal representatives of the Data Subjects are required to submit to Eastern Multi-Academy Trust a letter of authority to act on behalf of the Data Subject along with appropriate proof of the Data Subject's identity.
- 10.3 The Data Protection Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either:
- an investigation concerning national security.
 - the prevention or detection of crime; or
 - the apprehension or prosecution of offenders
- and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.
- 10.4 Every CCTV image disclosed is recorded in the CCTV Operating Logbook and contains:

- the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording.
- brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy.
- the crime reference number where relevant; and
- date and time the images were handed over to the police or other body/agency.

10.5 Requests of CCTV images for staff or student disciplinary purposes shall be submitted in writing to the Academy Principal in consultation with the Data Protection Officer.

10.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

11. COMPLAINTS PROCEDURE

11.1 Any complaints relating to the CCTV system should be directed in writing to the Academy Principal promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. If a complainant is not satisfied with the response, they may appeal to Eastern Multi-Academy Trust as per the Trust's Complaints Policy.

11.2 Complaints in relation to the release of images should be addressed to the Trust Operations Team as soon as possible and, in any event, no later than three months from the event giving rise to the complaint.

12. USEFUL LINKS

The Information Commissioner's Code of Practice can be found at:

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>