



Matrix
Academy Trust
EDUCATION WITHOUT EXCEPTION

CCTV Policy and Operational Procedures

Last review date:		September 2025	
Next Review date:		September 2028	
Review Cycle:		3 years	
Statutory Policy:		Yes	
Date	Version	Reason for change	Source
14.02.22	V2.0	Updates	Trust ICT Services
08.02.24	V3	Policy refresh and update	DPO
28.02.25	V3.1	Updates to Section 4 Roles and Responsibilities and Section 7 Storage and Retention	DPO
24.06.25	V3.2	Update to Section 5 – Number of Cameras	Trust ICT Services

Contents

1. Introduction3

2. Legislation3

3. Objectives of the CCTV Scheme.....3

4. Roles and Responsibilities4

5. Operation of the System5

6. Notification6

7. Storage and Retention.....6

8. Disclosure7

9. Training8

10. Monitoring and Review8

11. Data Protection Impact Assessments (DPIA)8

12. Complaints9

1. Introduction

The purpose of this policy and procedures is to provide assistance in the operation, management and regulation of the CCTV systems in place at academies in Matrix Academy Trust.

The CCTV systems used in our academies are owned and operated as follows:

Academy	Owned By	Operated By
Barr Beacon School	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users
Bloxwich Academy	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users
Dame Elizabeth Cadbury School	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users
Etone College	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users
Turves Green Boys School	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users
Smestow Academy	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users
Wednesfield Academy	Matrix Academy Trust	Trust IT Team, Headteacher, authorised users

2. Legislation

This policy takes account of the Trust's responsibilities under the following legislation and regulatory guidance:

[UK General Data Protection Regulation](#)

[Data Protection Act 2018](#)

[Human Rights Act 1998](#)

[European Convention on Human Rights](#)

[The Regulation of Investigatory Powers Act 2000](#)

[The Protection of Freedoms Act 2012](#)

[The Freedom of Information Act 2000](#)

[The Education \(Pupil Information\) \(England\) Regulations 2005 \(as amended in 2016\)](#)

[The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#)

[The School Standards and Framework Act 1998](#)

[The Children Act 1989](#)

[The Children Act 2004](#)

[The Equality Act 2010](#)

[Surveillance Camera Code of Practice \(2021\)](#)

These procedures should be read in conjunction with the Trust's Data Protection Policy, Freedom of Information Policy and Privacy Notices published on the Trust's websites.

3. Objectives of the CCTV Scheme

We have considered the privacy issues involved with using surveillance systems and have concluded that their use is necessary and proportionate to the needs we have identified.

At Matrix Academy Trust, the CCTV system has been implemented to:

- protect Trust buildings and assets, during and after operating hours;
- help discharge statutory responsibilities in relation to the safeguarding of pupils and staff;
- assist academies in implementing the Trust Behaviour and Anti-Bullying policies;
- reduce the incidence of crime and anti-social behaviour (including theft and vandalism);
- support the Police in efforts to deter and detect crime;
- assist in identifying, apprehending and prosecuting offenders;
- increase the personal safety of staff, pupils and visitors;
- protect members of the public; and
- ensure the academy's rules are respected so that the academy can be properly managed.

In line with those aims, any information captured by our CCTV systems is processed in performance of tasks carried out in the public interest, or where the academy has a duty to undertake a legal obligation. Special category data will only be processed where these lawful conditions are met, or explicit consent is sought from data subjects.

The CCTV systems are not intended for the following purposes, which are prohibited:

- covert surveillance, unless it is at the written request of a law enforcement agency with the appropriate authority;
- the ongoing monitoring individuals based upon their protected characteristics as specified by the Equality Act 2010; or
- any other purpose which is not consistent with the stated aims.

4. Roles and Responsibilities

Matrix Academy Trust

The Trust is the data controller for all personal data captured by its CCTV system. The Trust Board is responsible for:

- Agreeing proposed amendments and revisions to these CCTV procedures, in consultation with appropriate stakeholders and within the limits of our Data Protection Policy and relevant legislation;
- Approving Privacy Notices, which will include references to the CCTV systems where appropriate;
- Approving Data Protection Policy, which will include references to information recorded by the CCTV systems; and
- Making final decisions on complaints involving the administration of these procedures, and on data protection issues more generally.

The Data Protection Officer (DPO)

The DPO is responsible for:

- independently monitoring compliance with these CCTV procedures;
- coordinating any data protection impact assessments, as appropriate;
- reporting any findings and recommendations to the Governing Board for consideration;
- providing operational and strategic advice and support on data protection issues
- investigating any suspected data breaches relating to the CCTV system; and
- coordinating responses to subject access requests and freedom of information requests relating to information captured by the CCTV system.

The Data Protection Officer can be contacted at DPO@matrixacademytrust.co.uk

Headteacher/ Senior Leadership

The Headteacher, or Senior Leadership Team is responsible for:

- day-to-day leadership on data protection issues within the academy;
- liaising with the Data Protection Officer in relation to breach incidents or information rights requests relating to CCTV;
- ensuring staff in their academies receive appropriate and regular training on data protection;
- delegating access and use of CCTV systems to named staff within the academy as appropriate;

CCTV users (named staff in each academy)

- the day-to-day administration of the CCTV system, in accordance with these procedures;
- liaising with the Data Protection Officer in relation to breach incidents or information rights requests relating to CCTV;
- requesting exports of footage from Trust and academy staff where these are required to retained as evidence for to support other processes;
- storing exports of CCTV footage in secure locations accessible only by authorised users and in line with the Trust retention schedule.

The System Operators (ICT staff from the Trust and Academies)

The System Operator(s) for each academy is responsible for:

- the day-to-day administration of the CCTV system, in accordance with these procedures;
- ensuring routine performance monitoring, including random operating checks, takes place;
- supervising access to, and administration of, the CCTV system;
- regulating access to CCTV control areas, by satisfying themselves about the identity of the visitor(s) and the purpose of the visit(s) before any access is permitted;
- ensuring CCTV control areas are kept secure;
- Monitoring and auditing of logs which record who accesses the system and its recordings, and when;
- applying the retention policy to ensure information captured by the system is not stored longer than necessary.

In the event that a conflict of interest is identified, the Headteacher will nominate an alternative person to perform these duties on a case-by-case basis. These duties will be performed in accordance with our Data Protection Policy.

5. Operation of the System

The CCTV systems within the academy are implemented as follows:

Academy	Number of Cameras	Internal	External	Controlled From/By
Barr Beacon School	66	Yes	Yes	Trust IT Offices, named users devices
Bloxwich Academy	113 (Secondary) 20 (Primary)	Yes	Yes	Trust IT Offices, named users devices
Dame Elizabeth Cadbury School	109	Yes	Yes	Trust IT Offices, named users devices
Etone College	122	Yes	Yes	Trust IT Offices, named users devices
Turves Green Boys School	85	Yes	Yes	Trust IT Offices, named users devices
Smestow Academy	95	Yes	Yes	Trust IT Offices, named users devices
Wednesfield Academy	96	Yes	Yes	Trust IT Offices, named users devices

These systems will be operated 24 hours per day for every day of the year.

Some CCTV systems used in academies capture both images and audio footage.

The location of cameras is a key consideration in ensuring the CCTV scheme meets its objectives while minimising risks to individuals' privacy. Each academy has considered the following criteria when selecting locations for any additional cameras for installation:

- Spaces that do not have relevance to the scheme's purposes will be avoided where possible. This consideration should be given particular weight for spaces which are not part of the academy's premises (such as public pavements or neighbouring property).
- Cameras should be sited to ensure they can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- Cameras should be suitable for the location, bearing in mind the light levels and the size of the area to be viewed by each camera.
- Cameras should be positioned so they produce images of a consistent quality throughout the year (such that they are not obscured by plant growth during spring, for example).
- Cameras should be sited so they are secure and protected from vandalism.

Unless an immediate response is required, staff must not direct cameras at an individual, their property, or a specific group of individuals without authorisation being obtained for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Only authorised staff are permitted to view CCTV. Any requests to access footage from unauthorised staff, or members of the public, should be forwarded to the Data Protection Officer for review.

6. Notification

The academy will notify individuals that CCTV is in use by installing and maintaining signage at entrances to the academy's premises. Signage will:

- be clearly visible and readable;
- contain details of the organisation operating the system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as a simple website address, telephone number or email contact; and
- be an appropriate size depending on context such as whether they will be viewed by pedestrians or motorists.

7. Storage and Retention

Information captured by the CCTV systems will not be kept for longer than is necessary and for a time period that is relevant to the purposes we have established. As a minimum, CCTV footage will be retained for a period of 30 calendar days, however, in some instances clips, or extracts of footage relating to incidents may be kept for a longer period of time.

Recorded material will be stored:

- in a way that maintains the integrity of the information; and
- in a secure environment with restricted access and which is locked when not occupied by authorised staff.

The Data Protection Officer, and named staff at each academy, are authorised to access the system and its recordings where this is necessary. Other staff within the academy will be authorised by the Headteacher/Senior Leadership Team.

CCTV footage should only be downloaded/extracted from the system where it is necessary to support a purpose identified in Section 3 of this policy.

CCTV footage must not be recorded onto personal devices, for example by being recorded onto a mobile telephone. To share such footage in an unauthorised manner would constitute a data breach and lead to disciplinary procedures.

If a member of staff wishes to refer to CCTV footage in using the whistleblowing process, they should raise this within their expression of concern and ensure that this concern is raised within the time that such footage would be retained on the system, making clear the CCTV footage (i.e. date, time and location) which is being referred to. It is then the responsibility of the HR Director, or person addressing the whistleblowing, to take all necessary action to ensure that the relevant footage is recorded and stored securely.

8. Disclosure

Information captured by the CCTV systems is highly likely to constitute personal data, including special category data. Decisions to disclose this information externally may only be made by the Headteacher of the academy or the Trust Board in consultation with the Data Protection Officer.

Downloaded footage must not be shared without the written permission of the Headteacher/Senior Leadership Team and the DPO should be consulted in any such decision.

Requests will be considered on a case-by-case basis but such information may be disclosed to:

- the Police in order to support the detection and prevention of crime;
- the Health and Safety Executive, Local Authority, or any other statutory body charged with safeguarding children and young people in order to promote that safeguarding;
- individuals (or their authorised representatives) in response to a subject access request for their own personal data or where the requested information is subject to a court order; or
- the academy's insurance provider, where the information is required to support a claim for damages done to the insured property.

Where information is requested by external organisations, or an individual as an information rights request, this request should be made in writing. If a request is made verbally, the recipient should transcribe the request, so that this can be clarified by the Data Protection Officer. All requests will be reported to the Data Protection Officer.

Individuals wishing to access personal data captured by the Trust's CCTV systems, should submit their request to the Data Protection Officer by emailing DPO@matrixacademytrust.co.uk

Subject access requests should clearly state the date, approximate time and location footage may have captured an individual's personal data. If this is not provided as part of an initial request, the Data Protection Officer may ask the individual to clarify their request so the relevant records can be identified and reviewed.

In many cases, where the personal data of multiple individuals is captured in CCTV footage, the academy in consultation with the Data Protection Officer will be responsible for determining whether the disclosure of footage as part of an information rights request is reasonable.

The Data Protection Officer will consider whether disclosure of footage can be achieved in a manner that protects the rights and privacy of other individuals whose personal data may be contained in any clip/section of footage. Where disclosure of live/raw footage is not possible, the academy must consider whether the disclosure of still images taken from footage will allow an information rights request to be upheld.

The Trust CCTV systems do not support the redaction of live/raw clips of footage.

Footage may be viewed by the Police for the purposes of prevention and detection of crime, authorised Officers of the Police for supervisory purposes, authorised demonstration and training.

A record will be maintained by the System Operator of the release of recorded materials to the Police or other authorised applicants. A register will be made available for this purpose. Viewing of CCTV footage by the Police must be recorded in a centrally held log by the designated User or System Operator.

Should CCTV footage be required as evidence by the Police, a copy may be exported from the system and made available to the police using a approved secure transfer mechanism. Footage will only be released to the Police on the clear understanding that this remains the property of the school, and both the recorded material and information contained on it are to be treated in accordance with this document.

The school retains the right to refuse permission for the Police to pass footage obtained from Trust systems to any other person.

On occasions when a Court requires the release of an original recorded material, this request should be referred to the Data Protection Officer.

9. Training

All staff will be entitled to receive general training on data protection. Authorised users will require additional training before they are permitted access to the CCTV system. That will include:

- how to implement these procedures;
- that they are subject to a confidentiality duty and that it is a criminal offence to misuse surveillance system information;
- how to apply the arrangements set out in the Retention Schedule as they relate to information captured by the CCTV system;
- how to handle information securely;
- how to recognise both a subject access request and a freedom of information request, and what to do if such a request is received; and
- what to do if they receive a request for information from an official authority, such as the Police.

10. Monitoring and Review

The System Operator(s) will arrange for routine performance monitoring, including random operating checks. Such checks will consider, for example, whether:

- access restrictions are implemented appropriately and logs are kept up-to-date;
- signage is adequate; and
- recordings are disposed of in line with the Retention Schedule.

Additionally, independent monitoring may be carried out by the Data Protection Officer and/or the Trust Board. Such monitoring may take the form of a routine operating check, as above, but will also focus wider questions including whether:

- the system is addressing the needs and delivering the benefits that justify its use;
- the scheme complies with relevant legislation and codes of practice; and
- the technical, physical and organisational measures used are appropriate.

11. Data Protection Impact Assessments (DPIA)

The Trust follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure

the aim of the system is still justifiable, necessary and proportionate. The DPO will provide guidance on how to carry out the DPIA.

If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

12. Complaints

Complaints will be investigated in accordance with the Trust Complaints Policy.