CCTV Policy
2026

Contents

1. Statement of Intent

At Endeavour Learning Trust, we take our responsibility towards the safety of staff, visitors, and students very seriously.

To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our academies and its members, and to monitor any unauthorised access to our sites.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems and ensure that:

- We comply with all data protection legislation, including UK GDPR under the Data Protection Act 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing.
- Taking action to prevent a crime.
- Using images of individuals that could affect their privacy.

2. Purpose

The Purpose of this policy is to regulate the management, operation and use of the CCTV system at all academies within Endeavour Learning Trust.

CCTV systems are installed (both internally and externally) in all premises for the purpose of enhancing the security of each building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environment of each establishment during both the daylight and night hours each day.

CCTV surveillance is intended for the purposes of:

- protecting buildings and assets, both during and after school hours.
- promoting the health and safety of staff, students, and visitors as well as for monitoring student behaviour.
- preventing bullying.
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism).
- supporting the police in a bid to deter and detect crime.
- assisting in identifying, apprehending, and prosecuting offenders; and
- ensuring that the rules are respected so that each academy can be properly managed.

Each CCTV system is owned and operated by each academy within the Trust, the deployment of which is determined by the Senior Leadership Team within each academy.

The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the community.

Each sites CCTV is registered with the Information Commissioner under the terms of UK GDPR and the Data Protection Act 2018. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.

All CCTV operators are made aware of their responsibilities in following the CCTV Code of Practice, ensuring that safeguarding protocols are also followed. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

3. Scope

3.1 This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material.

3.2 Each academy complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use.

3.3 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound. Breaches of the code of practice by staff may lead to disciplinary action and possible criminal proceeding.

3.4 CCTV warning signs will be clearly and prominently placed at the main external entrance to each building.

3.5 CCTV does not have sound recording capability.

3.6 Signs will contain details of the purpose for using CCTV (see Appendix 1). In areas where CCTV is used, each academy will ensure that there are prominent signs placed within the controlled area.

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

3.8 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by each site, including Equality & Diversity Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment, Safeguarding Legislation, and other relevant policies, including the provisions set down in equality and other educational and related legislation.

3.9 This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g., race, gender, sexual orientation, national origin, disability etc.

3.10 Video monitoring of public areas for security purposes within education establishments is limited to uses that do not violate the individual's reasonable expectation to privacy. Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee or a student attending each site.

3.11 All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the Trust.

3.12 Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the UK General Data Protection Regulation under the Data Protection Act 2018.

4. Location of Cameras

4.1 Cameras are sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated.

4.2 Each academy will ensure that the location of equipment is carefully considered so that the images captured comply with current legislation.

4.3 Each academy will make every effort to position the cameras so that their coverage is restricted to their premises, which includes both indoor and outdoor areas.

4.4 CCTV will not be used in classrooms but in limited areas within the building that have been identified as not being easily monitored.

4.5 Members of staff will have access to details of where CCTV cameras are situated, except for cameras placed for the purpose of covert monitoring.

4.6 CCTV Video Monitoring and Recording of Public Areas may include the following:

- Protection of educational establishments and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services.
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas.
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms.
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control.
- Criminal Investigations (carried out by the police): Robbery, burglary, and theft surveillance.

5. Covert Monitoring

5.1 Each academy retains the right in exceptional circumstances to set up covert monitoring.

For example:

- Where there is good cause to suspect that an illegal or serious unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

5.2 In these circumstances, authorisation must be obtained beforehand from the Trust Chief Executive / Executive Head and Head of that establishment.

5.3 Covert monitoring may take place in classrooms when circumstances as above are satisfied. Covert monitoring used in classrooms will never be used to observe or assess a teacher's professional performance, or to contribute to capability proceedings.

5.4 Covert monitoring will cease following completion of an investigation.

5.5 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example, toilets.

6. Storage and Retention of CCTV Images

6.1 Recorded data will not be retained for longer than 31 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

6.2 Where data is retained for longer than 31 days an electronic file held on a secure central server where specific CCTV image/recordings are retained will be kept.

6.3 UK GDPR under the Data Protection Act does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage.

6.4 Therefore, retention will reflect each academy's purpose for recording information, and how long it is needed to achieve this purpose.

6.5 Appropriate security measures will be in place to prevent the unlawful or inadvertent disclosure of any recorded images. These measures in place include:

- The CCTV system being encrypted/password protected.
- Restriction of the ability to make copies to specified members of staff.
- A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images and reason, will be maintained by each site.

7. Access to CCTV Images

Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Head of the affected academy, the administration of the CCTV System may be delegated to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals who may differ from site to site but generally include the following individuals:

- Chief Executive/Exec Head/Head
- Senior Leadership Team
- DSL/DDSL
- Ops Manager
- IT Team
- Estates Team

8. Subject Access Requests (SARS)

8.1 Individuals have the right to request CCTV footage relating to themselves under UK GDPR under the Data Protection Act.

8.2 All requests should be made in writing to the Trust Data Protection Officer who can be contacted either by email or written communication. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: time, date, and location.

8.3 Each site does not have a facility to provide copies of CCTV footage but instead the applicant may view the CCTV footage if available.

8.4 Each site will respond to requests within 30 calendar days of receiving the request but if a request is received outside of the school term this may not be possible.

8.5 Each site reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

8.6 A fee may be charged where the request is excessive or unfounded.

9. Access and Disclosure of Images to Third Parties

9.1 There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police (see appendix 4 for the consent form for disclosure to the police) and service providers to each site where these would reasonably need access to the data (e.g., investigators).

9.2 If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, careful consideration must be given to exactly what the Court order requires. If there are any concerns as to the disclosure, then the Trust Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

9.3 Requests for images should be made in writing to the Trust Data Protection Officer who will then liaise with the appropriate establishment.

9.4 The data may be used within the academies discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

10. Responsibilities

The Head at each academy will ensure appropriate staff are responsible for the following:

- The use of CCTV systems is implemented in accordance with this policy.
- Oversees and co-ordinates the use of CCTV monitoring for safety and security purposes.
- Ensures that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g., an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Consider both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals and be mindful that no such infringement is likely to take place.
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy".
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only.
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Head.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.
- Ensure the CCTV system is reviewed annually using the checklist at Appendix 3.

11. Review of CCTV for Panel Use

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

As per para 9.4, the data may be used within the Trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. The footage, if deemed necessary, will be viewed by all parties and if required to formulate representations will be arranged in advance in good time. Such viewing is to ensure the interests of natural justice for the panel hearing.

Requests for access or disclosure will be recorded and the Headteacher will make the final decision as to whether recorded images may be released to persons other than the police following consultation if necessary with the Data Protection Officer.

12. Data Protection Impact Assessments and Privacy by Design

CCTV has the potential to be privacy intrusive. Each site will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.

13. Misuse of CCTV Systems

- The misuse of the CCTV system could constitute a criminal offence.
- Any member of staff who breaches this policy may be subject to disciplinary action.

14. Complaints

Any complaints relating to this policy or to the CCTV system operated by the Trust should be made in accordance with the Trust Complaints Procedure.

15. Policy Review

The Trust Data Protection Officer is responsible for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

16. Links with other policies

This CCTV policy is linked to:

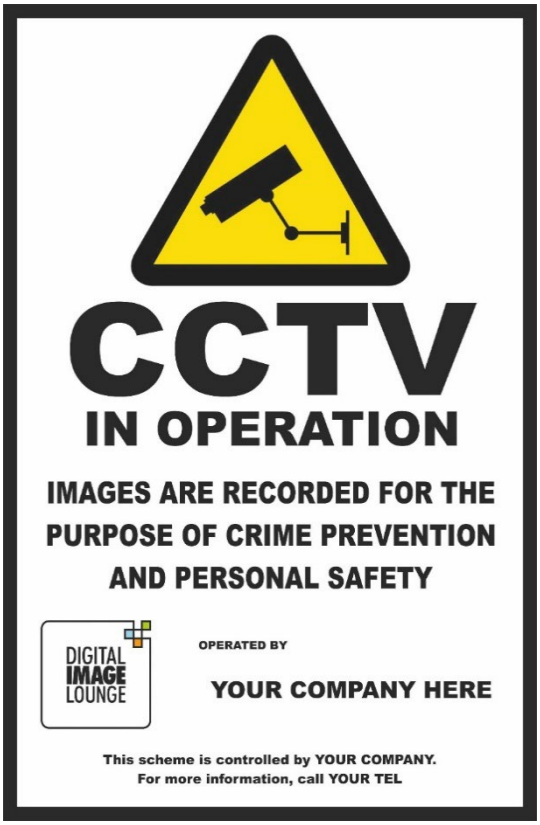
- Data Protection Policy
- Freedom of Information Policy
- Security Incident and Data Breach Policy
- Information Sharing Policy
- Data Protection Impact Assessment Policy
- Information Security Policy
- Acceptable use policy
- Safeguarding policy
- Privacy Notices

Appendix 1 – CCTV SIGNAGE

It is a requirement under UK GDPR and the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. Each site is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded.
- The purpose of using CCTV.
- The name of the academy.
- The contact telephone number or address for enquiries.



Appendix 2 – UK GDPR & Data Protection Act 2018

UK GDPR and the Data Protection Act 2018 principles.

1. Personal data shall be processed fairly and lawfully and shall not be processed unless:

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles, for further information refer to UK GDPR and the Data Protection Act 2018

Appendix 3 – Checklist

This CCTV system and the images produced by it are controlled by Endeavour Learning Trust who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement under UK GDPR and the Data Protection Act 2018).

The Endeavour Learning Trust have considered the need for using CCTV and have decided it is required for the prevention and detection of crime, safeguarding and the safety of students and all visitors to the Trust and its sites. The data may be used within the Trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures. We conduct an annual review of our use of CCTV.

	Checked (Date if appropriate)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.	Yes		
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required	Yes		
Staff will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.	Yes		
Cameras have been sited so that they provide clear images.	Yes		

Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Yes		
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	Yes		
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Yes		
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	Yes		
Except for law enforcement bodies, images will not be provided to third parties.	Yes		
The school knows how to respond to individuals making requests for copies of their own images. If unsure the data controller knows to seek advice from the Data Protection Officer/ Information Commissioner as soon as such a request is made.	Yes		
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Yes. (Daily checks)		
The school knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Data Protection Officer/ Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix 4 – Data Subject Access Request – Form (Police Requests)

For the purposes of this request Police are the third party and we would asked with the data subject consents to the disclosure of data from Endeavour Learning Trust in accordance with Police Form 0819B in that any special or personal data requested is supplied to the third party as soon as possible.

Data Subject's Information	
Name of the Data Subject	
Date of Birth	
Address where Data Subject attended school	
Third Party Information	
Name of the person requesting information on behalf of the Data Subject	
Address of the person requesting information on behalf of the Data Subject	
Personal Information Requested in relation to the Data Subject *Crime Reference Number for Request.*	
AUTHORISATION OF DATA SUBJECT	
I consent to the third party named in this consent form being provided with the special category or personal information specified in this form. *We require a signature to signify consent from the data subject to process their data and to ensure security measures relating that data are robust. Scanned copies will be accepted, provided the form is signed.*	Signed: Dated:

If you have any further queries regarding this form do not hesitate to contact our Data Protection Officer via phone on 01772 817904