CCTV Policy

Date Agreed with Trustees	**March 2022**
Date to be reviewed	**March 2025**

Contents

1. Policy Statement

The Endeavour Multi Academy Trust ("the Trust") uses Closed Circuit Television ("CCTV") within the premises of the Trust. The purpose of this policy is to set out the position of the Trust as to the management, operation and use of these CCTV systems.

This policy applies to all students, members of staff and visitors to the Trust's premises and all other persons whose images may be captured by the CCTV system.

This policy has been created with regard to the following statutory and non-statutory guidance -

- Endeavour MAT Data Protection Policy (2018).
- Home Office (2013) 'The Surveillance Camera code of Practice'.
- Information Commissioners Office (ICO 2017) 'Overview of the General Data Protection Regulation (GDPR).
- ICO (2017) 'In the Picture: A data protection code of practice for surveillance cameras and personal information'

2. Purpose and Justification of CCTV

2.1 The Trust uses CCTV for the following purposes -

- To provide a safe and secure environment for students, staff and visitors.
- To prevent the loss of, or damage to, the Trust's assets and or buildings.
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

2.2 The Trust has considered alternatives to using CCTV, such as additional regular inspections of its premises, but has concluded that such alternatives would be less effective and more costly. In particular, there are situations that require a rapid response if the risk to the security and safety of students, staff and visitors is to be minimised. CCTV is the best way for the Trust to achieve this.

2.3 The Trust reserves the right to use CCTV footage in connection with any disciplinary action or proceedings.

3. Description of System

3.1 The Trust uses fixed lens cameras on all its sites. Cameras are not equipped for sound recording.

4. Privacy Impact Assessment

4.1 Prior to the installation of any CCTV camera, or system, a Privacy Impact Assessment will be conducted by the Trust to ensure that the proposed installation is compliant with the legislation and the ICO guidance.

4.2 The Trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera, so as to avoid recording and storing excessive amounts of personal data.

5. Siting of Cameras

5.1 All CCTV cameras will be sited in such a way as to meet the purpose for which CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to students, staff and visitors.

5.2 Cameras will not be sited, as far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Trust will make all reasonable efforts to ensure that areas outside of the Trust premises are not recorded.

5.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

5.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing room or toilets, unless a specific Privacy Impact Assessment has been undertaken for the area.

6. Management and Access

6.1 The management of the CCTV system will be overseen by the Head of Premises and Estates for the Trust.

6.2 The viewing of live CCTV images will be restricted to access in schools and trust offices with explicit powers to view images, for the reasons set out above. Such access shall be granted by the Head of Premises and Estates, DPO, Trust CEO or Head Teacher, as appropriate.

6.3 Access to recorded images which are stored by the CCTV system will be restricted, and viewed only by Head of Premises and Estates, DPO, Trust CEO or Head Teacher.

6.4 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

6.5 The CCTV system is checked weekly by appropriate staff members in the Trust Schools to ensure that it is operating effectively.

7. Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose that they were originally recorded.

7.2 The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include -

- CCTV recording systems being located in restricted access areas.
- The CCTV system being encrypted/password protected.
- Restriction of the ability to make copies to specified members of staff. Such access will be granted as per 6.2 above.

7.3 A log of any access to the CCTV images, including time and date of access and a record of the individual accessing the images will be maintained by the Trust. This log is stored electronically, on each individual system.

8. Disclosure of Images to Data Subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images.

8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of section 9 of the Trust's Data Protection Policy.

8.3 When such a request is made, the Head of Premises and Estates or their appropriately nominated representative will review the CCTV footage, in accordance with the request.

8.4 If the footage contains only the individual making the request, then that individual may be permitted to view the footage. This must be strictly limited to that footage which contains only the images of the individual making the request. The Head of Premises and Estates or their representative must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals, then the Trust must consider whether -

- The request requires the disclosure of the images of individuals other than the requester, for example, whether the images can be distorted so as not to identify the individuals.
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

- If not, then whether it is otherwise reasonable, in the circumstances, to disclose those images to the individual making the request.

8.6 The DPO must record and keep securely records of all disclosures, which sets out -

- When the request was made.
- The process followed in determining whether the images contained third parties.
- The considerations as to whether to allow access to these images.
- The individuals that were permitted to view the images and when.
- Whether a copy of the images was provided and, if so, to whom, when and in what format.

All such requests shall be assessed in conjunction with the Trust's Freedom of Information and Data Protection Policies by the Trust Data Protection Officer. If deemed to fulfill all requirements, it shall than be passed to the Head of Premises and Estates for processing.

9. Disclosure of Images to Third Parties

9.1 The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

9.3 If a request is received from a law enforcement agency for disclosure of CCTV images, the Head of Premises and Estates must follow the same process as above in relation to subject access requests. Details should be obtained from the law enforcement agency as to exactly what they want the CCTV images for and any particular individuals of concern. This will then enable proper consideration to be given as to what should be disclosed and the potential disclosure of any third-party images.

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

The Trust follows the 12 guiding principles as set out by the ICO in it Code of Practice.

Appendix 1

Checklist

This CCTV system and the images produced by it are controlled by the Head of Premises and Estates who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose.

Endeavour MAT has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of students, staff and visitors. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (Date)	Checked (By)	Date of Next Review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	09/12/2019	DPO	Automatic renewal in line with ICO Registration renewal – July 2020
There is a named individual who is responsible for the operation of the system.	30/01/2022	DPO	30/01/23 or before if required
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.	30/01/2022	DPO	30/01/23 or before if required
A system has 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.	30/01/2022	DPO	30/01/23 or before if required
Cameras have been sited so that they provide clear images.	30/01/2022	DPO	30/01/23 or before if required
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	30/01/2022	DPO	30/01/23 or before if required
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).	30/01/2022	DPO	30/01/23 or before if required
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	30/01/2022	DPO	30/01/23 or before if required
The recorded images will only be retained long enough for any	30/01/2022	DPO	30/01/23 or before if required

incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.	30/01/2022	DPO	30/01/23 or before if required
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	30/01/2022	DPO	30/01/23 or before if required
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.	30/01/2022	DPO	30/01/23 or before if required
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	30/01/2022	DPO	30/01/23 or before if required

Appendix 2

Privacy Impact Assessment Template

1	Site details.
	WGSG/WGSB/SLS
2	Who will be captured on CCTV?
	Students / Staff / Visitors / Public
3	What personal data will be processed?
	Images
4	Why is the camera / system being installed? What is the issue that the Trust is trying to address? Is CCTV the best solution?
	Safety and security of Staff/Students/Visitors/School Buildings & Assets
5	What is the lawful basis for operating the CCTV system?
	Legal obligation, legitimate interests of the organization to maintain health and safety and to prevent crime.
6	Who is/are the named person(s) responsible for the system?
	Head of Premises and Estates

7	Describe the CCTV System.
	The site has cameras located within the grounds, both internally and externally. The cameras are high specification, fixed lens type with no sound recording ability, so that the images can be used for the purpose intended. Cameras have been situated in order to avoid capturing images which are not necessary. Signs indicating that CCTV is in operation are located at various places around the sites.
8	Set out the details of any sharing with third parties.
	CCTV footage may be provided to external parties such as the Police or through subject access requests. All recorded data is stored locally on internal hard drives located inside the NVR's
9	Set out the retention period of any recordings
	No longer than required for purpose to a maximum of 30 days.
10	Set out the security measures in place to ensure that recordings are captured and stored securely.
	CCTV footage is only accessible by authorised personnel and this access is password protected. The footage is stored is stored locally on internal hard drives located inside the NVR's
11	What are the risks to the rights and freedoms of individuals who may be captured on the CCTV footage?
	1. Identification of an individual. 2. Loss of data, if recordings are disclosed to a third party and not encrypted. 3. Misuse of data if accessed by unauthorised individual.

12	What measures are in place to address the risks identified?
	1. Identification will only be sought for justifiable reasons and by authorised personnel. 2. Data to be downloaded to a BitLocker encrypted USB stick or other secure transfer mechanism. 3. Authorised users are required to sign in using their personal login.

13	Have parents and pupils been consulted where appropriate, as to the use of the CCTV system?
	Yes – through policies and data privacy notices.
14	When will this P.I.A. be reviewed?
	As required, or with any changes to the CCTV system(s) in use but in any event at least annually as part of the review of this policy.

This template was approved by the Data Protection Officer

DPO

……

Date

……

Appendix 3

List of Role Holders with Authorised Access

Site	Role Holders with Authorised Access
EHO	Head of Premises and Estates Director of Data & Information Head of IT
SLS	Head Teacher Deputy Head Teacher Assistant Head Teachers ICT Managers Premises Manager Heads of Year
WGSG	Head Teacher Deputy Head Teacher Assistant Head Teachers Head Teacher's PA Support Manager KS 3/4/5 Sixth Form Admin Manager ICT Managers Site and premises staff Heads of Year
WGSB	Head Teacher Deputy Head Teacher Assistant Head Teachers Head Teacher's PA ICT Managers