Ernest Bevin Academy **CCTV Policy** 	
Strategic Aims **This policy aims to:** • Outline how and why Ernest Bevin Academy uses CCTV	
Responsibility: Head of Network and Learning Resource	**Date Approved**: Spring 2025
Approved by: Principal	**Review Date**: Spring 2026
Monitored by: Head of Network and Learning Resources	**Links to other Policies**: Privacy notice

Contents

1. Introduction

1.1 Ernest Bevin Academy has in place a CCTV surveillance system "the CCTV system" across its premises. This policy details the purpose, use and management of the CCTV system in the School and details the procedures to be followed in order to ensure that the School complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

1.2 The School will conform to the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the School will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

1.3 This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information' ("The Information Commissioner's Guidance").

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

2. CCTV System overview

2.1 The CCTV system is owned by *Ernest Bevin Academy, Beechcroft Road* and managed by the School and its appointed agents. The data controller for CCTV images held by Ernest Bevin Academy is United Learning Trust (ULT). ULT is registered with the Information Commissioner's Office (ICO). The registration number is Z7415170.

The Group's Data Protection Officer is responsible for ensuring that ULT complies with the Data Protection Law. The Data Protection Officer can be contacted at company.secretary@unitedlearning.org.uk or 01832 864538

The CCTV system operates to meet the requirements of the Data Protection Act 2018 and the Information Commissioner's Guidance.

2.2 Ernest Bevin Academy's designated Data Protection Lead is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.3 The CCTV system operates across the School. Details of the number of cameras can be given on request.

2.4 Clearly visible signs are placed at all pedestrian and vehicular entrances to inform staff, pupils, parents, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by the School and a 24-hour contact number for the Security Control Centre is provided, if appropriate.

2.5 The Data Protection Lead is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.6 Cameras are sited to ensure that they cover the School premises as far as possible. Cameras are installed throughout the School's sites including roadways, car parks, buildings (internal and external), within buildings and externally in vulnerable public facing areas.

2.7 Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screening or software masking will be utilised.

2.8 The CCTV system is operational and capable of being monitored 24 hours a day, every day of the year.

2.9 Any CCTV installation shall be subject to a Data Protection Impact Assessment. It will also comply with the policy and procedures within this document. The Data Protection Impact Assessment shall be appended to this policy and shared with the Central Office Data Protection Officer

3. Purposes of the CCTV system

3.1 The principal purposes of the School's CCTV system are as follows:

- for the prevention, reduction, detection and investigation of crime and other incidents;
- to ensure the safety of staff, children, visitors and members of the public; and
- to assist in the investigation of suspected breaches of school regulations by staff or students.

Cameras will be used to monitor activities within the college grounds, its car park and in the vicinity of the access gates to identify adverse activity occurring, anticipated, or perceived. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and school, together with its visitors only. Extra curriculum and activity clubs are not covered by this.

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

3.2 The CCTV system will be used to observe the school's buildings and areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

3.3 The school seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy as outlined in the Privacy Impact Assessment.

4. Monitoring and Recording

4.1 Cameras are only accessed by authorised members of the network services staff, who have access to the system (designated trained staff)
The captured footage can be accessed via Verkada Command or through a mobile app (where enabled). The School admins grant access using a role-based permissions model, enabling them to define the level of access users and groups of users have to the system. Access to the system is protected using stringent password requirements and session management. SAML/OAuth for single sign-on and 2-factor authentication is enabled (via SMS and authenticator applications). All access to the system is logged.

4.2 The footage captured by the camera is stored on the device. It may also be transmitted to the cloud for backup storage. Cloud data is stored using AES 256-bit encryption. Additional staff may be authorised by the Principal to monitor cameras on a view only basis.
Trained staff are as follows: DPL, SLT, HOY, and Pastoral Team.

4.3 A log shall be kept of requests to access recorded images by trained staff and whether any recorded images have been copied to support specific investigations. Information logged should include the name of staff, time and date of viewing, time and date of images reviewed, and a brief reason for viewing content (e.g. “incident in a corridor”) but should not contain names, whether any images have been copied and where they have been copied to.

Sharing via Command: Recorded history can be shared by email, and a URL gives them access via the permission management system, subject to role-based access and logging controls.
External Sharing by Verkada: For cloud storage, Verkada leverages as sub-processors Backblaze for the storage of cloud backups in the United States (US) and the European Union (EU), and AWS cloud services in Canada (CA) and Australia (AU).

4.4 The cameras installed shall provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images are accurate.

4.5 All images recorded by the CCTV System remain the property and copyright of United Learning. The recorded images are stored on the device.

4.6 The CCTV system should not be used to carry out lesson observations.

4.7 The use of cameras in areas where one would normally expect a degree of privacy should be clearly identified on the Privacy Impact Assessment. This would include cameras placed in, or looking into, toilets or changing areas.
Cameras should only be used in toilets or changing areas where there are full height cubicles, never in areas where it is possible to see people using the toileting facilities (excluding hand washing) or changing.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

5. Compliance with Data Protection Legislation

5.1 From 25 May 2018, the School will also comply with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provides that personal data shall be:

a. processed lawfully, fairly and in a transparent manner;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 All storage used for images, recorded or downloaded for investigations, must be in compliance with GDPR rules; on secure storage on premise or on cloud storage within the EEA

5.3 The existence of the School's CCTV system must be recorded in the Record of Data Processing Activities using United Learning's Education Information Portal (EIP).

6. Applications for disclosure of images

Applications by individual data subjects

6.1 Requests by individual data subjects for images relating to themselves "Subject Access Request" should be submitted in writing.

6.2 In order to locate the images on the School's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

6.3 Where the School is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual. Any decision to withhold the requested images must be referred to the Group's Data Protection Officer or his team as there are specific rules that must be adhered to when applying the exemptions contained in the Data Protection Act 2018.

Access to and disclosure of images to third parties

6.4 A request for images made by a third party should be made in writing.

6.5 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

6.6 All unexpected requests for CCTV images by a third party, including requests made by the police, should be referred to the School's Data Protection Lead in the first instance and if not available to the Group's Data Protection Officer or their team, who will advise on the application of any appropriate exemptions. Any third party request should be added to the EIP in the GDPR area under *third party request*s.

6.7 Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/ Business Partner, the Principal may provide access to CCTV images for use in staff disciplinary cases.

6.8 The Principal may provide access to CCTV images to Investigating Officers when sought as evidence in relation to staff discipline cases.

6.9 A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

7. Retention of images

7.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

7.2 The automatic deletion of data after the defined retention period should be checked on a half termly basis.

7.3 Where an image is required to be held in excess of the retention period referred to in 7.1, the Principal or their nominated deputy will be responsible for authorising such a request. A record of these stored images will be kept within the CCTV viewing log.

7.4 Exported images are kept on Verkada Command where they can be accessed via a shared link. This link has a default expiry period.

7.5 Access to retained CCTV images is restricted to the Principal and other persons as required and as authorised by the Principal. These individuals are: DPL

8. Complaints procedure

8.1 Complaints concerning the School's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Principal at Ernest Bevin Academy, Beechcroft Road. Any complaint will be handled in accordance with the School's complaints policy.

8.2 All appeals against the decision of the Principal should be made in writing to the *Chair of Governors*.

9. Monitoring Compliance

9.1 All staff involved in the operation of the School's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

9.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to have undertaken United Learning Data Protection training.

10. Policy review

10.1 The School's usage of CCTV and the content of this policy shall be reviewed annually by the Principal with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.