KING EDWARD VI FOUNDATION BIRMINGHAM

Educational excellence for our City

KING EDWARD VI ACADEMY TRUST BIRMINGHAM

CCTV Policy

Responsible Board/Committee	Audit Risk and Compliance Committee
Policy Type	Central Policy (Group A)
Policy Owner	Risk and Compliance
Statutory	Yes
Publish Online	Yes
Last Review Date	February 2026
Review Cycle	2 years This policy will not expire but will be reviewed as per its designated cycle. This policy remains effective whilst the review is taking place and will only become non-applicable once the updated version has been approved.
Next Review Date	March 2028
Version	2

1) Purpose

The Foundation and Academy Trust (collectively known as the Foundation) uses Closed-Circuit Television ("CCTV") and Internet Protocol (IP) Surveillance at its schools. The purpose of this policy is to set out the Foundation's position on the management, operation, and use of CCTV and IP Surveillance (collectively, Video Surveillance).

This policy applies to all members of staff and pupils across the Foundation, visitors to our individual premises, and all other persons whose images may be captured by the Video Surveillance system.

The Foundation uses Video Surveillance for the following purposes:

- To provide a safe and secure environment for pupils, members of staff, and visitors.
- To prevent the loss of, or damage to, Foundation buildings and/or assets; and
- To assist in the prevention of crime and to assist law enforcement agencies in identifying and apprehending offenders.

The legal bases for this use of CCTV are public task and vital interests (for safeguarding and safety of individuals), and legitimate interests in protecting Foundation property.

2) Roles and responsibilities

Headteachers are responsible for undertaking Data Protection Impact Assessments (DPIAs) in relation to any decision to implement CCTV or to change the way CCTV operates in the school.

Headteachers will delegate authority for the management and upkeep of any CCTV installations to an appropriate person in the school. This person will also maintain a CCTV asset register and will be responsible for decommissioning equipment appropriately at the end of its life, or when necessary, ensuring data leaks are prevented during this process.

The Data Protection Officer will review data protection impact assessments and approve or reject them based on compliance with relevant legislation.

The Risk and Compliance team will review this policy in line with its review schedule and will seek input from the Data Protection Officer during the review.

The School Data Protection Lead is responsible for keeping a record of CCTV images retained for investigation and will take advice from the Data Protection Officer on their retention.

3) Procedures

DESCRIPTION OF SYSTEM

Those schools that use Video Surveillance have fixed and moving cameras on-site. Cameras are not equipped for sound recording.

INSTALLATION AND SITING OF CAMERAS

The installation of CCTV must comply with the organisation's relevant financial regulations.

All Video Surveillance cameras will be positioned to meet the purpose for which the Video Surveillance is operated. Cameras will be placed in prominent positions where they are clearly visible to staff, pupils, and visitors.

Cameras will not be placed, so far as is reasonably practicable, in a way that records areas not intended to be the subject of surveillance. The Foundation will make all reasonable efforts to ensure that areas outside our premises are not recorded.

Signs will be erected to inform individuals that they are in an area where Video Surveillance is in operation. CCTV recording will therefore be overt and signposted.

Cameras will not usually be placed in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets. However, this will be permitted where there is a clear rationale, and a robust Data Protection Impact Assessment has been conducted and approved by the Data Protection Officer.

PRIVACY IMPACT ASSESSMENT

Before installing any new Video Surveillance camera or system, the Foundation will conduct a privacy impact assessment/data protection impact assessment to ensure the proposed installation complies with legislation and ICO guidance. Such assessments will acknowledge the need to take special account of children's privacy and will assess the safeguarding and safety reasons for implementing CCTV.

The Foundation will adopt a privacy-by-design approach when installing new cameras and systems, considering each camera's purpose to avoid recording and storing excessive amounts of personal data.

MANAGEMENT AND ACCESS

On a day-to-day basis, Video Surveillance will be operated by members of staff with appropriate delegated authority.

The viewing of Video Surveillance images will be restricted to members of staff with explicit powers to view images, for the reasons set out above.

Recorded images stored by the Video Surveillance system will be accessible only to members of staff with explicit powers to view them, for the reasons set out above.

No other individual will be permitted to view or access any Video Surveillance images unless in accordance with the terms of this policy and procedure regarding the disclosure of images.

The Video Surveillance systems should be checked weekly by the appropriate members of staff in schools to ensure they are operating effectively.

STORAGE AND RETENTION OF IMAGES

Information about your rights, privacy notices for children and adults, and retention periods is available on the Foundation website: https://kingedwardvifoundation.co.uk/gdpr/.

CCTV images will be stored to ensure confidentiality, integrity, and availability. Any images recorded by the Video Surveillance system will be retained only for as long as necessary for the purpose for which they were originally recorded.

Recorded images should be stored for no more than 7 days, or, in the case of IP Surveillance, for a 28-day recording cycle, unless there is a specific purpose for which they are retained for a longer period, such as a police investigation.

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

- Video Surveillance recording systems being in restricted access areas;
- The Video Surveillance system being encrypted/password protected; and
- Restriction of the ability to make copies to specified members of staff.

A log of any access to the Video Surveillance images, including the dates and times of access, and a record of the individual who accessed the images, should be maintained at each school.

DISCLOSURE OF IMAGES TO DATA SUBJECTS

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

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 the Foundation's Data Protection Policy.

When such a request is made, the appropriately nominated representative will review the Video Surveillance footage, in respect of relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request, the individual may be permitted to view it. This must be strictly limited to that footage which contains only images of the individual making the request. The nominated representative must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals, then the Foundation will 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 other 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.

A record must be kept, and held securely, of all disclosures which sets out:

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

DISCLOSURE OF IMAGES TO THIRD PARTIES

The Foundation will disclose recorded Video Surveillance images to third parties only where permitted by the Data Protection Legislation.

Video Surveillance images will be disclosed only to law enforcement agencies in accordance with the purposes for which the Video Surveillance system is in place.

If a request is received from a law enforcement agency for the disclosure of Video Surveillance images, the nominated person should follow a similar process as above for subject access requests. Details should be obtained from the law enforcement agency regarding exactly what they want the Video Surveillance images for and any individuals of concern. This will then enable proper consideration of what should be disclosed and of the potential disclosure of any third-party images.

The information above must be recorded in relation to any disclosure.

If a court orders disclosure of Video Surveillance images, this should be complied with. However, very careful consideration must be given to precisely what the court order requires. If there are any concerns about disclosure, the Data Protection Officer should be contacted in the first instance, and appropriate legal advice may be required.

MISUSE OF CCTV SYSTEMS

The misuse of Video Surveillance systems could constitute a criminal offence.

Any member of staff who breaches this policy and procedure may be subject to disciplinary action.

4) References, legislation, and guidance

This policy takes account of all applicable legislation and guidance, including:

- The UK General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (together the ‘Data Protection Legislation’)
- CCTV Code of Practice produced by the Information Commissioner’s Office
- Human Rights Act 1998