KING EDWARD VI FOUNDATION BIRMINGHAM

Educational excellence for our City

KING EDWARD VI ACADEMY TRUST BIRMINGHAM

CCTV Policy

Responsible Board/Committee	Academy Trust and Foundation Board
Policy Type	Central Policy (Group A)
Policy Owner	Risk and Compliance
Statutory	Yes
Publish Online	Yes
Last Review Date	January 2023
Review Cycle	2 years
Next Review Date	January 2025
Expiry Date	March 2025
Version	1

1. POLICY STATEMENT

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

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

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

- The 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
- Human Rights Act 1998

2. PURPOSE OF VIDEO SURVEILLANCE

The Foundation uses Video Surveillance for the following purposes:

- to provide a safe and secure environment for students, 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 assist law enforcement agencies in apprehending offenders.

3. DESCRIPTION OF SYSTEM

Those schools which use Video Surveillance have fixed and moving cameras on sites. Cameras are not equipped for sound recording.

4. SITING OF CAMERAS

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

Cameras will not be sited, so far as possible, in such a way as to record areas that are 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 within which Video Surveillance is in operation.

Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilet cubicles.

5. PRIVACY IMPACT ASSESSMENT

Prior to the installation of any new Video Surveillance camera, or system, a privacy impact assessment will be conducted by the Foundation to ensure that the proposed installation is compliant with legislation and ICO guidance.

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

6. MANAGEMENT AND ACCESS

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

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

Recorded images which are stored by the Video Surveillance system will be restricted to access by members of staff within the schools with explicit powers to view images, for the reasons set out above.

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

The Video Surveillance systems should be checked weekly by the appropriate members of staff in Schools to ensure that it is operating effectively.

7. STORAGE AND RETENTION OF IMAGES

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 only be stored for a period of seven days or in the case if IP surveillance a 28-day recording cycle, unless there is a specific purpose for which they are retained for a longer period, such as in the case of 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 time and dates of access, and a record of the individual accessing the images, should be maintained within each school.

8. 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, then the individual may be permitted to view the footage. 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 that 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.

9. DISCLOSURE OF IMAGES TO THIRD PARTIES

The Foundation will only disclose recorded Video Surveillance images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

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

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

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

If an order is granted by a Court for disclosure of Video Surveillance images, then this should be complied with. However, very careful consideration must be given to exactly what the Court

order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10. 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.