CCTV System Policy

Date of Issue: April 2021
Next Review Date: April 2022

Policy Cover Note

Title of the Policy	CCTV System Policy
Summary/Reason for bringing to Bord for Approval	New Policy
Statutory Requirement	No
Decisions to be made / recommendation on options	To be approved
Name of the author	Rachel Rowlamds
Date written	April 2021
Date for Review	April 2022
Policy/Procedure to be published on the trust website	Yes
Policy/procedure to be published on the Academy/Primary website	Yes
Amendments/Updates	

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Essa Foundation Academies Trust, hereafter referred to as 'the trust'.

The system comprises a number of fixed, dome and remote cameras located around the school site. All cameras are monitored via access to secure servers andare only available to selected senior staff (authorised users) on the Administrative Network.

This policy follows Data Protection guidelines and the Information CommissionersOffice CCTV code of practice (May 2015).

The policy will be subject to review annually to include consultation as appropriate with interested parties.

The CCTV system is owned by the trust.

2. Objectives of the CCTV scheme

- To protect the trust buildings and their assets
- To increase personal safety for staff, students and visitors and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the school

3. Statement of intent

The CCTV system will be registered with the Information Commissioner under the terms of the Data Protection Act and will seek to comply with the requirements ofthe Data Protection Act, GDPR and the Commissioner's Code of Practice.

The school will treat the system and all information, documents and recordingsobtained and used as data which are protected by the Act.

Cameras will be used to monitor activities within the trust grounds and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school, staff and students together with its visitors.

Authorised users are aware that static cameras are not to focus on private homes, gardens and other areas of private property.

Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without authorisation being obtained, as set out in the Regulation of Investigatory Power Act2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in theinvestigation of a specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

The planning and design has endeavored to ensure that the Scheme will givemaximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas ofcoverage.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the schoolCCTV.

4. Operation of the system

The day-to-day management will be the responsibility of the Business Manager, Facilities Manager and IT Manager during the day and the Sports Centre Manager out of hours and at weekends.

The main CCTV system will be operated 24 hours each day, every day of theyear.

Recordings are stored on hard drives for 28 days.

5. System functionality & Access

Access to the CCTV system will be strictly limited to the Business Manager, Facilities Manager, IT Manager and SLT within their designated area of work only.

Unless an immediate response to events is required, authorised staff must notdirect cameras at an individual or a specific group of individuals.

Visitors and other contractors wishing to enter areas of work where images arebeing displayed will be subject to particular arrangements as outlined below.

Authorised users must satisfy themselves over the identity of any other visitors who view images and the purpose of the visit. Where any doubt exists access will be refused.

The system may generate a certain amount of interest. It is vital that operationsare managed with the minimum of disruption. Visitors to the office where the CCTV is located must first obtain permission from the Business Manager or Facilities Manager

Any visit may be immediately curtailed if prevailing operational requirementsmake this necessary.

If out of hours emergency maintenance arises, the Operators must be satisfied ofthe identity and purpose of contractors before allowing entry.

Emergency procedures will be used in appropriate cases to call the EmergencyServices.

6. Liaison

Liaison meetings may be held with all bodies involved in the support of thesystem. (Business, Facilities, IT, SLT)

7. Monitoring procedures

- Camera surveillance may be maintained at all times.
- Server hard drives are used to record pictures.

8. Video CD / DVD procedures

In order to maintain and preserve the integrity of the disks, optical or magneticmedia used to record events from the hard drive and the facility to use them in any future proceedings, the following procedure for their use and retention must be strictly adhered to:

- Media required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store. If mediais not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence store.

- Recordings may be viewed by the Police for the prevention and detection of crimeor for supervisory purposes, authorised demonstration and training.

- A record will be maintained of the release of media to the Police or otherauthorised applicants.

- A register will be available for this purpose.

- Viewing of recordings by the Police must be recorded in writing and in the logbook. Requests by the Police can only be actioned under the Data Protection Act.

- Should a recording be required as evidence, a copy may be released to the Policeunder the procedures described in paragraph 8.1 of this Code. Media will only be released to the Police on the clear understanding that the media remains the property of the school, and both the media and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Police to pass to any other person the media or any part of the information contained thereon. On occasions when a Court requires the release of anoriginal recording this will be produced from the secure evidence store, complete in its sealed bag.

- The Police may require the school to retain the stored media for possible use asevidence in the future. Such media will be properly indexed and properly and securely stored until they are needed by the Police.

- Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Principal. In these circumstances the media will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in responseto a Court Order. A fee can be charged in such circumstances: £10 for subject accessrequests; a sum not exceeding the cost of materials in other cases.

9. Breaches of the code (including breaches of security)

Any breach of the Code of Practice by school staff will be initially investigated bythe Principal, in order for them to take the appropriate disciplinary action.

10. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried outby the Business Manager and the Facilities Manager.

11. Complaints

Any complaints about the school's CCTV system should be addressed to the Principal.
Complaints will be investigated in accordance with Section 9 of this Code.

12. Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personaldata" relate) with a right to data held about themselves, including those obtained byCCTV.

Requests for Data Subject Access should be made to the Principal.

13. Public information

Copies of this Code of Practice will be available to the public from the School Office.

14. Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the school.
- The viewing of images is not open to visitors except by prior arrangement and goodreason.
- Liaison meetings may be held with the Police and other bodies.
- Recording media will be used properly, indexed, stored and destroyed afterappropriate use.
- Recordings may only be viewed by authorised school officers and the Police.
- Media required as evidence will be properly recorded, witnessed and packagedbefore copies are released to the police.
- Recordings will not be made available to the media for commercial use orentertainment.
- Media no longer required will be disposed of securely by incineration.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the corporatepolicies and procedures and must be logged.
- Any breaches of this code will be investigated by the Principal.

15. Monitoring

EFAT is responsible for auditing the CCTV System policy and procedures.