North Essex Multi-Academy Trust

# CCTV System Policy

| | |
|---|---|
| **Last reviewed:** | June 2020 |
| **Next review due:** | June 2022 |
| **Ratified Trust Board:** | 9 June 2020 |
| **Designated Postholder:** | Data Protection Officer |

**This policy is for implementation in all Academies within NEMAT.**

## 1. Introduction

1.1 The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at North Essex Multi-Academy Trust (NEMAT), hereafter referred to as 'the Trust'.

1.2 The system comprises several fixed, dome and remote cameras located around the school site. All cameras are monitored via access to secure servers and are only available to authorised users.

1.3 This Policy follows Data Protection and GDPR guidelines and the Information Commissioner's Office CCTV code of practice: In the picture: A data protection code of practice for surveillance cameras and personal information.

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

1.4 the Policy will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the school.

## 2. Objectives of the CCTV scheme

(a) To protect the school buildings and their assets

(b) To increase personal safety and reduce the fear of crime

(c) To support the Police in a bid to deter and detect crime

(d) To assist in identifying, apprehending and prosecuting offenders

(e) To protect members of the public and private property

(f) To assist in managing the school

(g) To assist in the behaviour management of students

(h) CCTV can be used to 'monitor the movements and behaviour of individuals

## 3. Statement of intent

3.1 The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the DPA and GDPR.

3.2 Cameras will be used to monitor activities within the school 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, together with its visitors.

3.3 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 Act 2000.

3.5 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 the investigation of a

specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

3.6 The planning and design have endeavoured to ensure that the Scheme will give maximum 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 of coverage.

3.7 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 school CCTV.

## 4. Operation of the system

4.1 The Scheme will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the Senior Leadership Team, IT Support team and the Site Manager during the day and the Site Team out of hours and at weekends.

4.3 The main CCTV system will be operated 24 hours each day, every day of the year.

4.4 Recordings are stored on hard drives for approximately 2-3 weeks, this is dependent on factors such as the quality setting, hard drive space, number of cameras on the box, movement in the footage etc and are wiped at expiry or retained for investigatory purposes if required.

## 5. System functionality & Access

5.1 The System Manager will check and confirm the efficiency of the system daily and that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV system will be strictly limited to the staff for whom SLT, have deemed it necessary for the fulfilment of their role and within their designated area of work only.

5.3 Unless an immediate response to events is required, authorised staff must not direct cameras at an individual or a specific group of individuals.

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

5.5 Operators must satisfy themselves as to the identity of any other visitors who view images and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be logged and signed off before recordings are viewed.

5.6 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted.

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

5.8 Access to the servers (physically or remotely) is limited to the Operators via unique accounts which are password protected. Server rooms are secured both during the working day and when not manned.

5.9 Other administrative functions will include maintaining recordings and hard disc space, filing and maintaining occurrence and system maintenance logs.

## 6. Monitoring procedures

6.1 Camera surveillance may always be maintained .

6.2 Server hard drives are used to record pictures both continuously and on motion.

## 7. Video CD / DVD procedures

7.1 In order to maintain and preserve the integrity of the disks, optical or magnetic media 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 media is 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.

7.2 Recordings may be viewed by the Police for the prevention and detection of crime in accordance with the DPA and GDPR, they must provide the proper authorised documentation. All such viewings must be recorded in a register.

7.3 A record will be maintained of the release of media to the Police or other authorised applicants. A register will be available for this purpose.

7.4 Should a recording be required as evidence, a copy may be released to the Police under 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 an original recording this will be produced from the secure evidence store, complete in its sealed bag.

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

7.6 Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Headteacher. 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 response to a Court Order.

## 8. Breaches of the code (including breaches of security)

8.1 Any breach of the Code of Practice by school staff will be initially investigated by a senior manager in line with the Trust's Discipline and Dismissal Procedure.

8.2 Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

## 9. Assessment of the scheme and code of practice

9.1 Performance monitoring, including random operating checks, may be carried out by the System Manager and the Site Manager.

## 10. Complaints

10.1 Any complaints about the school's CCTV system should be addressed to the Headteacher.

## 12 Access by the Data Subject

12.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. However, they must provide specific dates and times as viewing CCTV by members of the public should be limited to still shots not video where other individuals could be identified.

12.2 Requests for Data Subject Access should be made to the Headteacher.

## 13 Public information

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

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 good reason.

• Liaison meetings may be held with the Police and other bodies.

• Recording media will be used properly, indexed, stored and destroyed after appropriate use.

• Recordings may only be viewed by authorised School Officers and the Police.

• Media required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.

• Recordings will not be made available to the media for commercial use or entertainment.

• Any stored Media no longer required will be disposed of securely as per our Retention and Deletion Policy.

• Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the corporate policies and procedures and must be logged.

• Any breaches of this code will be investigated by a senior manager. An independent investigation will be carried out for serious breaches.

• Breaches of the code and remedies will be reported to the Headteacher.

Related Policies

This policy links with our Behaviour, Child Protection, Retention and Deletion, Data Protection Policies and the Staff Discipline and Dismissal Procedure.