The Four Stones Multi Academy Trust
CCTV Policy

Version Control
Policy author: Jessica Bushell
Policy approved by: Finance, Audit and Risk Committee
Next policy review date: Spring 2022

Version	Date	Details
1.0	18th March 2020	Policy written
2.0	1st Sept 2021	General updates-eg replacing 'associate headteacher' with 'headteacher'

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 the schools in The Four Stones Multi Academy Trust (MAT).

1.2 The CCTV system is owned by the MAT.

1.3 All cameras are monitored by the Network Managers. The Trust Estates and Facilities Manager and the Site Managers can also access the CCTV system as the site team are directly involved in the security of the school site.

1.4 This policy follows the General Data Protection Regulation (GDPR) guidelines.

1.5 Operation of the MAT's CCTV Policy will be reviewed by the trustees.

2. **Objectives of the CCTV Scheme**
(a) To protect the MAT's 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 disciplining offenders
(e) To protect members of the public and private property.

3. **Statement of Intent**
3.1 The CCTV system will be registered with the Information Commissioner's Office (ICO), if necessary, under the terms of the GDPR and will seek to comply with the requirements of the ICO's Code of Practice 2008.

3.2 The MAT will treat the system and all information, documents and recordings obtained and used as data which are protected by the ICO's Code of Practice 2008.

3.3 Cameras will be used to monitor activities within access and entrances to the schools and the car parks, internal communal areas, internal corridors and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the schools, together with its visitors.

3.4 Staff have been instructed to ensure cameras are not able 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 an authorisation being obtained for directed surveillance to take place, 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. Recorded materials will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Recorded materials will never be released to the media for purposes of entertainment.

3.6 The planning and design has endeavoured to ensure that the CCTV system 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 CCTV system.

4. **Operation of the CCTV System**
4.1 The system will be administered and managed by the Network Managers, in accordance with the principles and objectives expressed in this policy.

4.2 The day-to-day management will be the responsibility of the Network Manager.

4.3 In the absence of the Network Manager, the headteacher has the authority to direct another member of the IT technical support team to operate the CCTV system.

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

5. **Operational Control**
5.1 The Network Managers will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

5.2 The Data Protection Officers will ensure that all staff involved with the operation of the CCTV system are properly trained and fully understand their roles and responsibilities in respect of data protection issues e.g. rights of individuals in relation to their recorded images. Training records will be maintained accordingly.

5.3 In an emergency, access to the viewing monitors will be strictly limited to selected senior and administrative staff together with those directly involved in the security of the school.

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

5.5 Staff, visitors and others entering areas with CCTV viewing monitors will be subject to particular arrangements as outlined below.

5.6 Authorised staff must satisfy themselves over the identity of any other visitors and the purpose of their visit. Where any doubt exists the CCTV images must be turned off.

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

5.8 If an emergency arises out of hours, permission must be obtained from the Network Manager to view or process recorded material. In the absence of the Network Manager, permission can be obtained from the Trust Estates and Facilities Manager or Site Manager.

5.9 Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.

5.10 Incidents involving the Emergency Services must be notified to the Network Manager, Trust Estates and Facilities Manager or Site Manager.

6. **Liaison**
Liaison meetings will be held as required with all staff involved in the support of the system.

7. **Monitoring Procedures**
7.1 Camera surveillance may be maintained at all times.

7.2 Pictures will be continuously recorded or when activated by movement.

7.3 No covert monitoring will be undertaken until the circumstances have been considered by, and written authorisation obtained from the Trust Estates and Facilities Manager and headteacher.

7.4 Covert surveillance activities of law enforcement agencies are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000.

7.5 Prior to any request for covert surveillance to be considered, the applicant must be able to justify the request as being exceptional for the following reasons:
- the monitoring relates to behaviour, not to contract performance
- it is carried out to investigate a suspected criminal activity or malpractice
- informing staff is likely to prejudice the above purpose and certain standards for covert monitoring are complied with.

The standards relating to covert monitoring are satisfied if:
- specific criminal activity has been identified;
- a need to obtain evidence by covert monitoring is established;
- following assessment, it is concluded that informing employees would prejudice the gathering of evidence;
- a time period for monitoring has been identified; and
- the provisions of RIPA are complied with.

At the conclusion of an investigation, all covert cameras are to be removed from their location(s) and all data destroyed as soon as possible.

8. **Recorded Material Procedures**
8.1 In order to maintain and preserve the integrity of the recorded material used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
(i) Each item of recorded material must be identified by a unique mark.
(ii) Before use each item on which images will be recorded must be cleaned of any previous recording.
(iii) The person making the recording shall register the date and time of recorded material insert, including recorded material reference.
(iv) Any recorded material required for evidential purposes must be sealed, witnessed, signed by the Network Manager, dated and stored in a separate, secure recorded material store. If recorded material 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 Network Manager, dated and returned to the evidence material store.
(v) If the recorded material is archived the reference must be noted.

8.2 Recorded materials may be viewed by the Police for the prevention and detection of crime, authorised officers of the Police for supervisory purposes, authorised demonstration and training.

8.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register will be made available for this purpose.

8.4 Viewing of recorded materials by the Police must be recorded in writing and in a log book.

8.5 Should recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1(iv). Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the school, and both the recorded material and information contained on it are to be treated in accordance with this document.

8.6 The school retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material this will be produced from the secure recorded material store, complete in its sealed bag.

8.7 If the Police require the school to retain the stored recorded materials for use as evidence in the future, such recorded materials will be properly indexed and properly and securely stored until they are needed by the Police.

8.8 Applications received from outside bodies (e.g. solicitors) to view or release recorded materials will be referred to the Trust Estates and Facilities Manager and headteacher. In these circumstances recorded materials 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.

9. **Record Keeping/Incident Logs**
The MAT will maintain adequate and comprehensive records relating to the management of the system and incidents.

10. **Retention of Data**
10.1 There are no specific guidelines about the length of time data images should be retained. Consequently, the period of retention will be determined locally, will be documented and understood by those operating the system and will be for the minimum period necessary to meet the objectives of the CCTV system. A period of 30 days is considered adequate unless determined otherwise (see 10.2 below).

10.2 Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.

10.3 Measures to permanently delete data should be clearly understood by persons that operate the system. These may be achieved by means of regular rotation of video tape(s) to ensure old data is overwritten or adjusting the image quality on disc based systems to ensure data is overwritten after a set period.

10.4 Systematic checks should be carried out to ensure the deletion regime is strictly followed.

11. **Breaches of the Policy (including breaches of security)**
Any breach of the policy by the MAT's staff will be initially investigated by a member of the senior leadership team, to determine disciplinary action, if necessary, and to make recommendations on how to remedy the breach.

12. **Assessment of the CCTV System**
An annual assessment will be undertaken by the Network Manager to evaluate the effectiveness of the CCTV system.

13. **Complaints**
Any complaints about the CCTV system should be made in accordance with the MAT's 'Complaints Procedure'.

14. **Access by the Data Subject**
14.1 The General Data Protection Regulation provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. If the individual is not the focus of the footage i.e. they have not been singled out or had their movements tracked then the images are not classed as 'personal data' and the individual is not entitled to the image under the provisions of Subject Access – General Data Protection Regulation.

14.2 Requests for subject access requests should be made to the data protection officer. Please refer to the MAT's 'Data Protection Policy'.

15. **Public Information**
Copies of this policy will be available to the public from the school office.

16. **Further Information**
Information in respect of data protection issues may be obtained from the Council's Data Protection/Freedom of Information Officer (tel: 01905 763763). The Information Commissioners website www.ico.gov.uk will contain the most up to date information and should be consulted on a regular basis to ensure all elements of this policy continue to reflect current guidance.