CCTV System Policy

Documentation Information			
Reviewed By	Directors	**Responsibility**	Network Manager
Last Reviewed	Nov 2009, Mar 2014, Jan 2017, May 2018	**Next Review**	May 2020
Review Cycle	biennial	**Ratified by Directors**	May 2018

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 LiFE Multi Academy Trust and its schools, hereafter referred to as 'the trust'.

1.2 The system comprises a number of static and dome cameras located around the school sites. All cameras can be monitored by selected staff who have been given authorisation by the Executive Head. They are not watched continually and have been installed to prevent and deter crime, vandalism and to monitor student behaviour.

1.3 This Code follows General Data Protection Regulation (GDPR) guidelines.

1.4 The Code of Practice will be subject to review as required by law or biennial and will include consultation as appropriate with interested parties.

1.5 The CCTV system and data are owned by the trust.

2. Objectives of the CCTV system

- To protect the trust buildings and assets of those buildings
- To increase personal safety 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 through monitoring student behaviour (if required)

3. Statement of intent

3.1 The CCTV system will be registered with the Information Commissioner under the terms of GDPR and will seek to comply with the requirements both of the GDPR and Commissioner's Code of Practice.

3.2 The trust will ensure that they treat the system, all information contained on the system, documents, recordings obtained and used as data in accordance with GDPR, which are protected by the Act.

3.3 The system installed is compliant with the GDPR, Human Rights Act and Regulatory Investigation Powers Act.

3.4 Cameras will be used to monitor activities across the trust to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the users of the trust facilities, including pupil misbehaviour.

3.5 Cameras are focussed on strategically placed areas across the schools in the trust. Private property is protected by privacy settings.

3.6 Materials of knowledge secured as a result of CCTV will not be used for any commercial purpose. Information transferred to CD/DVD (or other appropriate media) will only be used for the investigation of a specific crime or incident. Should this material ever require being released to the media, this would only be allowed with the written authority of the police; if this was required by them, as part of a police investigation.

3.7 The planning and design has endeavoured to ensure that the 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.

3.8 Warning signs, as required under the GDPR, have been placed at areas across schools within the trust.

3.9 The CCTV system has only been setup to record video footage. The audio record feature that are available on cameras has been switched off. The trust does not therefore record any audio feeds.

4. Operation of the System

4.1 The system will be administered and managed by the Network Manager for the Trust who reports to the Executive Headteacher/CEO), in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the ICT team during the day and the Premises Officer out of hours and at weekends, and holidays.

4.3 The control room will only be staffed by authorised personnel.

4.4 The CCTV system will be operated 24 hours a day, every day of the year (where possible).

5. Control Rooms

5.1 The Control Rooms will be locked at all times when not manned.

5.2 The ICT team will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

5.3 Unless an immediate response to events is required, or in anticipation of an event occurring, staff in the CCTV control rooms must not direct cameras at an individual or a specific group of individuals.

5.4 Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangements as outlined below.

5.5 Control Room Operators must satisfy themselves of the identity of any visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be denied.

5.6 If out of hours emergency maintenance arises, the Control Room operators must be satisfied as the identity and purpose of contractors before allowing entry.

5.7 Other administrative functions will include maintaining recording media and hard disc space, filing and maintaining occurrence and system maintenance logs.

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

6. Liaison

6.1 Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring Procedures

7.1 Camera surveillance may be maintained at all times.

7.2 Monitoring software is installed and used by authorised persons for out of hours monitoring.

7.3 Information is held on the hard drive for a period of no more than 14 days or if required longer for further investigations. If information is required for evidence purposes it will be transferred to appropriate recording media and stored appropriately.

8. CD/DVD/Recording Media Procedures

8.1 In order to maintain and preserve the integrity of the media 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:

(1) each record must be identified by a unique mark (ie incident, location and date with time stamp)

(2) before using each recording media must be cleaned of any previous recording

(3) the controller shall register the date and time of recorded insert, including the reference

(4) A recording required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure store. If the record 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 secure storage, if the record is archived, the reference must be noted.

8.2 Recording media may be viewed by designated operators and the Police for the prevention and detection of crime.

8.3 A record will be maintained of the release of records to the Police or other authorised applicants.

8.4 Viewing of records by the Police must be recorded in writing in the log book. Requests by the Police can only be actioned under the relevant section of the GDPR.

* Documents are usually stored on site at the related school where an incident took place (or in the UK) and these records are only stored in line with legislation.

8.5 Should a record be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1(4) of this Code. Records will only be released to the Police on the clear understanding that the record remains the property of the trust, and both the record and information contained on it are to be treated in accordance with this code. The trust also retains the right to refuse permission for the Police to pass on the record or any part of the information contained therein to any other person. On occasions when a Court requires the release of an original record this will be produced from the secure store, complete in its sealed police bag.

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

8.7 Applications received from outside bodies (e.g. solicitors) to view or release records will be referred to the Executive Headteacher/CEO. Charges maybe requested to cover the costs of producing the material.

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

9.1 Any breach of the Code of Practice by trust staff will be initially investigated by an investigating officer appointed by the Executive Headteacher/CEO, in order for the trust to take the appropriate action.

9.2 Any serious breach of the Code of Practice including breaches of the Code of Practice by the Head of School will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach, by the governing body.

10. Assessment of the system and the Code of Practice

10.1 System monitoring will include random checks by authorised staff.

10.2 The Code of Practice will be reviewed in line with legislation updates.

10.3 Regular reviews of the systems operation will take place and any necessary changes in procedure or camera sighting/position will be implemented.

11. Complaints

11.1 Any complaints about the trust's CCTV system should be addressed to the Executive Headteacher/CEO.

11.2 Complaints will be investigated in accordance with appropriate sections of this code.

12. Access by the Data Subject

12.1 The GDPR provides Data Subjects (individuals to whom 'personal data' relates) with a right to view data held about themselves, including that obtained by CCTV.

12.2 Requests for Data Subject Access should be made by application to the Executive Headteacher/CEO.

13. Public Information

13.1 Copies of the Code of Practice will be available to the public but must be requested in writing from the trust.

14. System Maintenance

14.1 The system will be subject to regular maintenance and repairs.

14.2 Equipment and recordings may be viewed by personnel authorised to undertake installation and maintenance of the CCTV systems.

14.3 Such viewing will be restricted to that necessary for system work