Joseph Leckie Academy

CCTV Policy

Approved by JLA Trust Board:	09/2021
Last reviewed on:	10/2022
Next review due by:	10/2023

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 our Academy.

- The CCTV system is owned and operated by the Academy, and its deployment is determined by the Principal.
- The system comprises a number of fixed and dome cameras located around the Academy site. CCTV footage is only available to designated employees – members of the Site Team and members of the Senior Leadership Team (SLT).
- All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained by the Academy Buildings and Health and Safety Manager in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.
- Any changes to CCTV monitoring will be subject to consultation with employees and the Academy Trustees.
- This policy follows Data Protection Act 2018 (DPA) and General Data Protection Regulations (GDPR) 2016 guidelines.
- The Academy's CCTV System is registered with the Information Commissioner under the terms of the DPA 2018 and the GDPR 2016. This policy outlines the Academy's use of CCTV and how it complies with UK and other relevant legislation.

1.2 This policy shall be reviewed regularly; we aim to conduct reviews no later than every two years. If new equipment is introduced a review will be conducted.

2. Scope

2.1 The CCTV system has been installed by the Academy with the primary purpose of reducing the threat of crime, protecting our premises and helping to ensure the safety of all of our students visitors and employees while consistent with respect for the individuals' privacy. The purpose of our CCTV system is to:

- To protect students, visitors and employees against harm to their person and/or property.
- To increase a sense of personal safety and reduce the fear of crime.
- To protect the Academy buildings and assets.
- To support the police in preventing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders.
- To assist in managing the Academy.
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence.
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against employees or students and assist in providing evidence to managers and/or to a member of an employee or student against whom disciplinary or other action is, or is threatened to be taken.

2.2 The CCTV system will not be used:

- To provide recorded images for the world wide web.
- To record sound other than in accordance with the section on covert recording.
- For any automated decision taking

2.3 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

3. Statement of Intent

3.1 The CCTV system will be registered with the Information Commissioner under the terms of the DPA 2018 and will seek to comply with the requirements of the GDPR 2016 and the Information Commissioner's Code of Practice.

- The Academy will treat the CCTV system and all information, documents and recordings obtained and used as data which are protected by the Act.
- Cameras will be used to monitor activities within the Academy 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 students, employees and visitors.
- Static cameras will not focus on private homes, gardens and other areas of private property.
- Unless an immediate response to events is required, cameras must not be directed at an individual, their property or a specific group of individuals, without an authorisation being obtained, as set out in the Regulation of Investigatory Power Act 2000.
- Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Tapes will never be released to the media for purposes of entertainment.
- The planning and design has endeavoured to ensure that the CCTV 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.
- 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 Academy CCTV.

4. Covert Monitoring

4.1 The Academy may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances authorisation must be obtained from the Principal

a. Covert monitoring must cease following completion of an investigation.
b. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

5. Operation of the System

5.1 The CCTV system will be administered and managed by the Principal, in accordance with the principles and objectives expressed in the Information Commissioners Code of Practice. The management of the CCTV system will be the responsibility of both the SLT and the Buildings and Health and Safety Manager during the day and the Site Team out of hours and at weekends. The CCTV controls and hardware devices will only be accessed by SLT, the Buildings and Health and Safety Manager and the Site Team. The CCTV system will be operated 24 hours each day, every day of the year.

6. Controls and Hardware

- The Site 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.
- Access to the CCTV controls and hardware devices will be strictly limited to the SLT, Buildings and Health and Safety Manager and the Site Team.
- Contractors required to access the CCTV controls and hardware devices for maintenance purposes will be subject to particular arrangement as outlined below.
    - The Site Team must satisfy themselves over the identity of any contractors wishing to access the CCTV controls and hardware devices and the purpose of the visit. Where any doubt exists, access will be refused. Details of all visits and contractors will be recorded on the sign in screen, located in reception.
    - It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Contractors must first obtain permission from the Buildings and Health and Safety Manager, and must be accompanied by a member of the Site Team throughout the visit.
    - Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
    - If out of hours' emergency maintenance arises, the Academy must be satisfied of the identity and purpose of contractors before allowing entry.
    - A visitor's record will be maintained at Academy reception. Full details of contractors including time/date of entry and exit will be recorded.
    - Emergency procedures will be used in appropriate cases to call the Emergency Services.

7. Access to CCTV Images

7.1 Access to recorded images will be restricted to those employees authorised to view them and will not be made more widely available.

8. Storage & Retention of CCTV Images

8.1 Recorded data will not be retained for longer than is necessary, up to a maximum of 30 days. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

8.2 All retained data will be stored securely on the network with restricted access. See the Records Management Policy and Schedule for further details.

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

9.1 Any breach of the Code of Practice by Academy employees will be initially investigated by the Principal, in order for him/her to take the appropriate disciplinary action. 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.

10. Complaints

10.1 Complaints and enquiries about the operation of CCTV within the Academy should be directed to the Principal in the first instance.

11. Further information and Associated Policies

11.1 For further information on CCTV and its use is available from the following:

- CCTV Code of Practice (published by the Information Commissioners Office)
- For further guidance from the ICO visit their website www.ico.org.uk

- Data Protection Act 2018
- General Data Protection Regulation 2016

11.2 This policy should be read alongside:

- Information Governance Strategy
- Information Risk and Security Policy
- Data Protection Policy
- Confidentiality Policy
- Information Rights Policy
- Records Management Policy and Schedule
- Incident Management Policy
- Subject Access Request Policy
- Consent to Use Personal Data Guidance
- Impact Levels and Protective Marking Guidance