

CCTV policy

1 Purpose & scope

- 1.1 Closed-circuit television (CCTV) images are monitored and recorded by Cabot Learning federation (CLF) for the purposes of the prevention and detection of crime and pupil/student, staff and public safety.
- 1.2 This Policy applies to all teaching and support staff employed by CLF, students, parents/carers and all users of CLF premises.

2 Introduction

- 2.1 This Policy ensures the effective and compliant management, operation and use of CCTV across CLF. The system comprises of a number of fixed cameras located around our academy sites.
- 2.2 This Policy follows UK General Data Protection Regulation (UK GDPR) laws and the Information Commissioners CCTV Code of Practice. The Policy will be subject to regular review taking into account changes in the law, recommended best practice and any relevant comments from interested parties.
- 2.3 The Principal of each academy is accountable for ensuring CCTV on their premises is operated in line with this Policy.

3 Objectives of the CCTV Policy

- 3.1 The objectives of the Policy are as follows:
 - To protect the federation's buildings and assets.
 - To increase personal safety and reduce the fear of crime.
 - To deter criminals from targeting CLF sites.
 - To assist the Police in identifying, apprehending and prosecuting offenders.
 - To protect members of the public.
 - To assist in managing and running the federation and its Academies.

4 Statement of Intent

- 4.1 CLF will treat the CCTV systems used on its sites, and all information, documents and recordings obtained and used, as personal data which are protected by the UK GDPR and Data Protection Act 2018.
- 4.2 Cameras will be used to monitor activities within the federation, 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 well-being of the federation's students, employees, visitors and users of its premises.
- 4.3 Cameras must not capture images overlooking private homes, gardens and other areas of private property.
- 4.4 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals (Directed Surveillance), without

written authorisation being obtained from a member of the Executive Team or Principal, as set out in the Regulation of Investigatory Power Act 2000.

- 4.5 Materials or knowledge secured as a result of CCTV must not be used for any commercial purpose. Where images need to be released to the media for use in the investigation of a specific crime, disclosures must be made by the Police, not CLF. Images must never be released to the media for purposes of entertainment.
- 4.6 The planning, design and implementation of CCTV has endeavoured to ensure that it gives 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.
- 4.7 Signs and notices must be prominently displayed to ensure individuals are informed that CCTV equipment is in operation and the purposes for which it is being used.

5 Operation of the System

- 5.1 CCTV will operate 24 hours each day, every day of the year.
- 5.2 CCTV will be administered and managed in accordance with the principles and objectives expressed in the Information Commissioners CCTV Code of Practice and this Policy.
- 5.3 Access to images must be strictly controlled. Routine viewing of recorded images is to be limited to:
 - Members of the Executive Team;
 - Academy Principals and Vice Principals;
 - Operations Managers;
 - Building Services Managers or in their absence a nominated deputy;
 - IT Support Staff; and
 - The CLF Data Protection Officer (DPO).
- 5.4 When circumstances require, Principals, Vice Principals, Operations Managers and the DPO will have authority to allow recorded images to be viewed or downloaded. All instances where images are viewed and / or downloaded must be recorded in a Register. Viewing of images by the Police or any third parties must also be recorded in the Register.
- 5.5 Typical examples of where the use of CCTV images would be in keeping with this Policy are to:
 - Help police or law enforcement investigate a crime or apprehend or prosecute an offender or suspected offender.
 - Assist in the application of health and safety practices, including the investigation into personal accidents, slips and trips.
 - Investigate a bullying incident.
 - Assist in the investigation of an alleged theft by a pupil.
 - Support an investigation of trespassing or unauthorised access to a building or premises.
 - Investigate a physical or verbal assault.

- Identify witnesses to an alleged crime or a student, staff or public safety incident.

This list is not exhaustive and other purposes may be or become relevant.

6 Image Control

- 6.1 As a general rule, images must be retained for a minimum of one calendar month and, where possible, 60 days before they are deleted or overwritten.
- 6.2 Cameras must be pointed and focused on fixed points agreed in advance by the Principal of each academy. Only Principals can authorise the modification of camera positions in response to a particular event or circumstances that is deemed to require surveillance.
- 6.3 The CCTV system must not be used for covert surveillance unless specifically directed by authorised law enforcement agencies.
- 6.4 Should images be required as Police evidence; disclosures must be made in line with the CLF Data Protection guidance entitled “Handling Disclosures of Personal Information”.
- 6.5 Applications received from outside bodies (e.g., solicitors, insurers or local authorities) to view or release images must be referred to the DPO. Again, any disclosures made must be in line with the CLF Data Protection guidance entitled “Handling Disclosures of Personal Information.”

7 Breaches of the Policy (including breaches of security)

- 7.1 Any breach of this Policy must be initially investigated by the Principal or a member of the Executive Team (or an appropriate nominated senior member of staff).
- 7.2 Serious breaches of this Policy will be subject to an independent investigation, carried out to determine if disciplinary action is necessary and to make recommendations on how to minimise the chance of similar breaches occurring in the future.

8 Complaints

- 8.1 Any complaints about the federation’s use of CCTV should be addressed in writing to the Principal or member of the Executive Team who will ensure an investigation is carried out. Where the complainant disagrees with the outcome of the investigation, they may escalate their concerns via the Grievance Procedure (for staff) or the Complaints Procedure (for non-staff).

9 Access to Images by the Data Subject or Their Representative(s)

- 9.1 The UK GDPR and Data Protection Act 2018 provides Data Subjects (the individuals to whom personal data relate) with the right to access copies of the personal data held about them, including those obtained by use of CCTV. All Subject Access Requests must be referred to the DPO immediately.

10 Public information

- 10.1 Copies of this Policy will be published on the Cabot Learning Federation website.

11 Summary of Key Points

- This Policy relates to CCTV equipment which is controlled by Cabot Learning Federation.
- Images are recorded and monitored for the prevention and detection of crime and pupil/student, staff and public safety.

- Images must not be kept for longer than is necessary.
- Images must only be viewed by Authorised Staff and the Police.
- Images required by the Police as evidence must be properly recorded, witnessed and packaged before copies are released.
- Images must not be made available to the media for commercial purposes or entertainment.
- Any breaches of this Policy will be investigated by the academy Principal where the breach took place. An independent investigation will be carried out for serious breaches.