Academies Trust

CCTV Policy

Approved by Trust Board: 13 July 2022

Applicable from: 1 October 2022

Review Date: 1 September 2025

This document represents a Trust-wide approach which is approved by the Trust Board for use in all sites operated by the Co-op Academies Trust.

If any significant changes to this policy are proposed at a local level, these must be referred to the Trust's JCNC through the Head of HR. When Trust colleagues are working on Co-op Group premises (for example, 1 Angel Square), the Co-op Group policies will apply.

Co-op Academies Trust

CCTV Policy

Contents	Page Number
1 – Introduction	3
2 - Statement of Intent	3
3 - Scope	3
4 - Roles and Responsibilities	4
5 - Siting the Cameras	4
6 - Covert Monitoring	5
7 - Operating Standards	5
8 - Storage and Retention of CCTV Images	6
9 - Access to CCTV Images	6
10 - Subject Access Requests	7
11 - Access to and Disclosure of Images to Third Parties	8
12 - Freedom of Information Requests	9
13 - Complaints	9
14 - Further Information and Guidance	9
15 - Review	9
Appendix 1 – Checklist of Operation	8
Appendix 2 – CCTV Signage	10

Closed Circuit Television (CCTV) Policy

1. Introduction

1.1 The purpose of this document is to regulate the management, operation and use of CCTV systems in our academy.

1.2 Each of our sites will tailor this policy in order to set out the purpose of using CCTV, what information will be recorded, who will have access to this information and how this information will be stored and disposed of.

2. Statement of Intent

2.1 The Trust, as the data controller, will ensure compliance with the law relating to data protection, namely the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy includes the principles governing the processing of personal data. It also seeks to ensure compliance with privacy law. It considers best practice as set out in the guidance issued by the Information Commissioner in regard to video surveillance. The Trust will only use CCTV where it is necessary in pursuit of a legitimate aim (see 2.2) and only if it is proportionate to that aim.

2.2 The Trust seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors and contractors, as well as its property and premises. It therefore deploys CCTV to:

- promote a safe community and to monitor the safety and security of its premises, staff and students;
- assist in the prevention, investigation, and detection of crime;
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by staff, students, visitors and contractors and, where relevant and appropriate, in the investigation of complaints.

2.3 CCTV data will not be used in any aspect of performance management, unless with the written consent of the employee concerned.

3. Scope

3.1 This policy applies to CCTV systems in all parts of the Trust.

3.2 This policy does not apply to any webcam systems that may be located in meeting rooms, classrooms or lecture theatres, which are used to assist audio visual equipment.

3.3 This policy applies to all staff, and any contractors or agents who operate, or supervise the operation of any CCTV system on behalf of the Trust.

4. Roles and Responsibilities

4.1 The Data Protection Officer for the Trust has overall responsibility for this policy but has delegated day to day responsibility for overseeing its implementation to the GDPR Ambassador within each academy. All relevant members of staff have been made aware of the policy and have received appropriate training.

4.2 The GDPR Ambassador, in consultation with the Data Protection Officer, the Headteacher, the IT team and the premises team, is responsible for ensuring that the CCTV system, including camera specifications for new installations, complies with the law and best practice referred to in clause 2.1 of this policy. Where new surveillance systems are proposed, the GDPR Ambassador will consult with the Data Protection Officer to determine whether a data protection impact assessment is required.

4.3 Only suitably competent contractors with the relevant knowledge and experience will be employed to install and maintain the equipment.

4.4 The GDPR Ambassador is responsible for the evaluation of locations where live and historical CCTV images are available for viewing. The list of such locations and the list of persons authorised to view CCTV images is maintained by the GDPR Ambassador.

4.5 Changes in the use of any CCTV system can be implemented only in consultation with the GDPR Ambassador and the Data Protection Officer.

4.6 The GDPR Ambassador will be responsible for completing a checklist of operation on an annual basis or as and when any changes to the CCTV system takes place.

5. Siting the Cameras

5.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (see 2.2) and care will be taken to ensure that reasonable privacy expectations are not violated. Each site will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act. Cameras will be regularly checked to ensure they have not been moved or tampered with in any way.

5.2 Each site will make every effort to position cameras so that their coverage is restricted to their premises, which may include outdoor areas.

5.3 CCTV cameras are installed in such a way that they are not hidden from view. CCTV warning signs will be clearly and prominently placed so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. Signs will be placed at the main entrances to the site, including the academy/site gates and entrances to the buildings, at

the entrance of the CCTV zone and within the controlled area. Signs will contain details of the purpose for using CCTV (see appendix 1).

5.4 CCTV will not be used in classrooms with the exception of the agreed use of equipment designed to provide professional development opportunities, which will only be used with the permission of all involved.

5.5 The planning and design of the system has endeavoured to minimise any invasion of privacy and ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will fully meet this brief or detect every single incident taking place in the areas of coverage.

5.6 The contact point for queries about CCTV around the academy/site should be available to staff, students and members of the public during normal business hours. Any employees staffing the contact point must be familiar with this policy and the procedures to be followed if an access request is received from a data subject or a third party.

6. Covert Monitoring

6.1 Covert monitoring (monitoring that takes place without the individual's knowledge) should not normally be considered, and should only be used in <u>exceptional</u> circumstances, for example:

i) Where there is good cause to suspect that criminal activity or equivalent malpractice which may constitute gross misconduct has taken place;

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording;

iii) Where there is no other reasonable, less intrusive means of achieving the same purpose.

6.2 In these circumstances written authorisation <u>must</u> be obtained from the Regional Director before allowing such an operation to take place. Unless the Regional Director is instructed otherwise (e.g. in a police investigation), members of the JCNC and the Data Protection Officer will also be informed confidentially about any plans for covert monitoring.

6.3 Any decision to engage in covert recording will be documented, including the reasons.

6.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets or changing areas.

6.5 Covert monitoring must cease following completion of an investigation.

7. Operating Standards

7.1 The operation of the CCTV system will be conducted in accordance with this policy.

7.2 Quality of recorded images

7.2.1 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended.

7.2.2 Recording features such as the location of the camera and/or date and time reference must be accurate and maintained.

7.2.3 Consideration should be given to the physical condition in which the cameras are located, e.g. additional lighting or infrared equipment may be required in poorly lit areas.

7.2.4 Cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept.

7.2.5 As far as possible, cameras must be protected from vandalism to ensure they remain in working order.

8. Storage and Retention of CCTV images

8.1 Recorded data will not be retained for longer than is necessary to meet the purposes of recording them. Data storage is automatically managed by the CCTV system which overwrites historical data in chronological order to produce an approximate 21 days rotation.

8.2 Provided there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the 21 day retention period.

8.3 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.

8.4 All retained data will be stored securely and access will be limited (see 9.1).

9. Access to CCTV images

9.1 Access to the control room and to any recorded images will be restricted to the following personnel, and will not be made more widely available:

- the Trust's Data Protection Officer
- the academy's GDPR Ambassador
- the Headteacher / Head of School / Executive Headteacher

- persons specifically authorised by the GDPR Ambassador or the Data Protection Officer
- maintenance engineers (upon producing appropriate ID)
- police officers where appropriate (upon producing appropriate ID and documentation); and
- any other person with statutory powers of entry.

9.2 A list of staff authorised to view images from its CCTV system will be held by each academy.

9.3 CCTV monitors will not be visible from outside the control room.

9.4 Where authorised persons access or monitor CCTV images on workstations, they must ensure that images are not visible to unauthorised persons. Workstation screens must always be locked when unattended.

9.5 A CCTV Operating log will be maintained showing when CCTV footage has been accessed and reviewed; this will detail:

- Person reviewing the footage
- Time, date and location of the footage being reviewed
- Purpose of reviewing the recordings
- Whether the footage has been downloaded and the reasons why
- The crime reference number where relevant
- Date and time the images were handed over and to whom
- The location of the downloaded footage

9.6 Downloaded CCTV images will be shown only to persons authorised to view them or to persons who otherwise have a right to access them.

10. Subject Access Requests (SARs)

10.1 Recorded images, which directly or in combination with other factors enable a data subject to be identified, are considered to be the personal data of the individuals whose images have been recorded on the CCTV system.

10.2 Data subjects have the right to request CCTV footage relating to themselves under the Data Protection Act.

10.3 Requests can be made verbally or in writing in accordance with the Data Subject Request Policy.

10.4 Any member of staff receiving such a request should immediately alert the GDPR Ambassador who will liaise with the data subject to obtain sufficient information to enable the footage relating to them to be identified and isolated. For example, date, time and location.

10.5 Subject to paragraph 10.6, the academy will respond to requests without undue delay and at the latest within one calendar month of receiving the written request.

10.6 The period for responding to the request may be extended by a further two months where necessary, considering the complexity and number of the requests. The GDPR Ambassador, in consultation with the Data Protection Officer will notify the data subject of any such extension within one month of receipt of the request together with the reasons.

10.7 The academy reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation. Where images of other individuals are on the CCTV footage their permission will be sought before access is allowed or the footage redacted to protect their identity

11. Access to and Disclosure of Images to Third Parties

11.1 Third party requests for access will usually only be considered in line with the UK GDPR and the Data Protection Act in the following categories:

- legal representative of the data subject (subject to paragraph 11.2);
- law enforcement agencies including the police;
- disclosure required by law or made in connection with legal proceedings;
- trade union representative (subject to paragraph 11.2); and
- colleagues or individuals tasked with investigating allegations against members of staff, student exclusions, complaints investigations and related proceedings.

11.2 Legal representatives and trade union representatives of the data subject are required to submit to the GDPR Ambassador a letter of authority to act on behalf of the data subject along with appropriate proof of the data subject's identity.

11.3 The GDPR Ambassador will disclose recorded images to law enforcement agencies including the police once in possession of a form certifying that the images are required for either:

- an investigation concerning national security;
- the prevention or detection of crime; or
- the apprehension or prosecution of offenders;

and that the investigation would be prejudiced by failure to disclose the information.

11.4 Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

11.5 In the case of 10, 11.3 or 11.4 images may be held beyond the usual deletion period pending appropriate approvals being sought and provided.

11.6 Every CCTV image disclosed is recorded in the CCTV Operating Log (see 9.5).

11.6 Requests for CCTV by colleagues or individuals tasked with investigating allegations against members of staff, student exclusions, complaints investigations and related proceedings shall be submitted to the GDPR Ambassador.

12. Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with the Trust's Freedom of Information Policy.

13. Complaints

13.1 Complaints and enquiries about the operation of CCTV within the academy should be directed to the Headteacher / Head of School in the first instance.

13.2 Failure of authorised operators/staff to comply with the requirements of this policy will lead to disciplinary action under the Trust's disciplinary procedure.

14. Further Information and Guidance

Further information and guidance on CCTV and its use is available from the following sources:

- Video Surveillance Guidance issued by the Information Commissioners Office https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/
- Guidance regarding Data Protection Impact Assessments https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 1998
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Crown Prosecution Service – www.cps.gov.uk

15. Review

This policy will be reviewed every 3 years, or sooner if required due to changes in legislation or statutory guidance.

Appendix 1 – CCTV Signage

It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded.

Each site is to ensure that this requirement is fulfilled.

Every CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or email address of the systems operators for enquiries (this will either be the school or if monitored externally the details of the provider)
- The signage must include a pictorial image identical to the one shown below

Please note that whilst every sign should include the details specified above, it is not a requirement to have a sign positioned at every camera. There should be clear signs on entry to the building and in appropriate areas of the site i.e. the dining hall.

Signs should be placed at an appropriate height and should be of a sufficient size so that they are easy to read.