



Academies Trust

CCTV Policy

Approved by Trust Board on 10 December 2020

Applicable from 11 December 2020

Review Date: December 2023

This document represents a Trust-wide which is approved by the Trust Board for use in the Trust's academies.

It is the responsibility of individual academies to insert information in to the document so that it is relevant to local circumstances and practice, whilst not removing the key principles contained within it, prior to the policy being noted by Local Governing Bodies.

If any 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), Co-op policies will apply.

Co-operative Academies Trust
Policy on the use of CCTV

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

Closed Circuit Television CCTV Policy Document for Connell Co-op College

1. Introduction

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

- 1.1 Connell uses closed circuit television (CCTV) images to reduce crime and monitor the college buildings in order to provide a safe and secure environment for pupils, staff and visitors, to prevent the loss or damage to property and to assist in the investigation of accidents, incidents and near misses.
- 1.2 The system comprises of 32 fixed and 4 dome cameras
- 1.3 The system does not have sound recording capability.
- 1.4 The CCTV system is owned and operated by the college and the deployment of which is determined by the college's leadership team, in line with this policy which has been agreed with trade union representatives.
- 1.5 The introduction of, or changes to, CCTV monitoring will be shared with local trade union representatives, staff and the college community.
- 1.6 The college's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act 1998. This policy outlines the college's use of CCTV and how it complies with the Act.
- 1.7 All authorised operators and employees approved to access images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the college's data controller in their responsibilities as part of the requirements of this policy document, the college's safeguarding policies and procedures, e-safety information and the Data Protection Act. All employees are aware of the restrictions in relation to storage of, access to, and disclosure of recorded images and sound. Failure to adhere to these requirements, could lead to disciplinary action.

2. Statement of Intent

- 2.1 The college complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The checklist of operation (appendix 1) is adapted from this document. Further information is available at:

<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

- 2.2 CCTV warning signs will be clearly and prominently placed at all external entrances to the college, including main staff/student and visitor entrances and college gates, as coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see appendix 2). In areas where CCTV is used, the college will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.
- 2.3 The planning and design of the system has endeavoured to minimise any invasion of privacy and ensure that the Scheme 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.
- 2.4 CCTV data will not be used in any aspect of performance management, unless with the written consent of the employee concerned.

3. Siting the Cameras

- 3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The college 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.
- 3.2 The college will make every effort to position cameras so that their coverage is restricted to the college's premises, which may include outdoor areas.
- 3.3 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 (see IRIS Protocol at appendix 3 for more detail).

- 3.4 Members of staff upon request will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring (see section 4).
- 3.5 Only suitably competent contractors with the relevant knowledge and experience will be employed to install and maintain the equipment.

4. Covert Monitoring

- 4.1 Covert monitoring should not normally be considered, and should only be used in exceptional circumstances, for example:
- i) Where there is good cause to suspect that a criminal activity or equivalent malpractice which may constitute gross misconduct;
 - ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances written authorisation must be obtained from the Director of the Trust or Chair of the Trust Board before allowing such an operation to take place. Unless the Director of the Trust is instructed otherwise (e.g. in a police investigation), members of the JCNC will be informed confidentially about any plans for covert monitoring.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 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.

5. Storage and Retention of CCTV images

5.1 Recorded data will not be retained for longer than is necessary than to meet the purposes of recording them, and will be deleted/erased appropriately and in line with approved procedures for the college as documented in appendix 1. 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.

5.2 All retained data will be stored securely. Access will be limited to named operators/staff only (see appendix 1) whose access is authorised by the Headteacher / Principal.

6. Access to CCTV images

- 6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.
- 6.2 A list of staff authorised to view Images from this CCTV system will be held by the college.
- 6.3 A log will be maintained of when CCTV footage is accessed and reviewed (name of reviewer, date & reason).

7. Subject Access Requests (SAR)

- 7.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.
- 7.2 All requests must be made in writing to the Principal / Headteacher. Individuals submitting requests for access will have to provide sufficient information to enable the footage relating to them to be identified & isolated. For example, date, time and location.
- 7.3 The college will respond to requests within 40 calendar days of receiving the written request and fee.
- 7.4 At the Trust's discretion, a fee of £10 may be charged per Subject Access Request.
- 7.5 The college 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.

8. Access to and Disclosure of Images to Third Parties

- 8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the college where these would reasonably need access to the data (e.g. investigators).
- 8.2 Requests should be made in writing to the Principal / Headteacher / Governing Body.
- 8.3 The data may be used within the Trust's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the college should be directed to the Principal / Headteacher in the first instance.

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

10. Further Information & Guidance

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

- Data Protection Code of Practice for surveillance cameras and personal information 2015 (published by the Information Commissioners Office www.ico.org.uk):
<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>
- The Government's Surveillance Camera Code of Practice 2013:
<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>
- Guidance on conducting a privacy impact assessment:
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
- 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

11. Review

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

Appendix 1 – Checklist of Operation

The College's CCTV system and the images produced by it are controlled in line with our policy, our data controller will notify the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).

The College has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of users of the site. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Action	Date	Print & Signed	Review Date
The name of the individual responsible for the operation of the system is: Jack Brien	29/03/22	Jack Brien	29/03/25
The reason for using CCTV has been clearly defined and installation / use of cameras is the best solution.	29/03/22	Jack Brien	29/03/25
The system is checked to verify it produces clear images which the law enforcement bodies (usually the police) can use to investigate crime, these can easily be taken from the system when required.	29/03/22	Jack Brien	29/03/25
Staff and members of the College community are consulted about the proposal to install and or continued use of CCTV equipment.	29/03/22	Jack Brien	29/03/25
Cameras have been sited so that they provide clear images and limit the opportunity to be tampered with.	29/03/22	Jack Brien	29/03/25
The potential impact on individuals' privacy has been identified and taken in to account in the use of the system.	29/03/22	Jack Brien	29/03/25
Cameras are located in the following areas: All communal areas,	29/03/22	Jack Brien	29/03/25

All external areas			
Cameras have been positioned to avoid intentionally capturing the images of persons not visiting the premises.	29/03/22	Jack Brien	29/03/25
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	29/03/22	Jack Brien	29/03/25
Images from this CCTV system are securely stored in Facilities office and access is limited to the following authorised persons: Jack Brien (Connell) Emma Soper [Connell] Aiden Sinclair (Connell) Robert Jarvis (Connell)	29/03/22	Jack Brien	29/03/25
Recorded images will be deleted after 30 days, unless they form part of an incident under investigation.	29/03/22	Jack Brien	29/03/25
Procedures are in place to respond to the police or individuals making requests for access to data held.	29/03/22	Jack Brien	29/03/25
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	29/03/22	Jack Brien	29/03/25

Appendix 2 – CCTV Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded.

The College is to ensure that this requirement is fulfilled.

The 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 where this is not obvious
- 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)
- Your signage must include a pictorial image identical to the one shown below

