

The **co-operative** academies trust

Policy on the Use of Closed Circuit Television (CCTV)

**Approved by Trust Board 19 July 2016
Applicable from 01 December 2016**

This document represents a Trust-wide policy 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 where indicated so that it is relevant to local circumstances and practice, whilst not removing any content 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	5
7 - Subject Access Requests	6
8 - Access to and Disclosure of Images to Third Parties	6
9 – Complaints	6
10 - Further Information & Guidance	7
11 – Review	7
Appendix 1 – Checklist of Operation	8
Appendix 2 – CCTV Signage	10
Appendix 3 – IRIS Protocol	11

Closed Circuit Television CCTV Policy Document for (Insert) Academy

1. Introduction

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

- 1.1 (INSERT NAME OF ACADEMY) uses closed circuit television (CCTV) images to reduce crime and monitor the academy 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 **(insert how many)** number of fixed* and dome* cameras (*DELETE AS APPLICABLE).
- 1.3 The system has/does not* have sound recording capability. (*DELETE AS APPLICABLE)
- 1.4 The CCTV system is owned and operated by the academy (OR STATE ALTERNATIVES if ownership or operation is for example shared) and the deployment of which is determined by the academy's leadership team, in line with this policy which has been agreed with trade union representatives.
- 1.5 The CCTV is monitored centrally from (INSERT LOCATION) by (INSERT NAME/POSITION OF DATA CONTROLLING OFFICER OR 3rd PARTY IF REMOTELY MONITORED).
- 1.6 The introduction of, or changes to, CCTV monitoring will be shared with local trade union representatives, staff and the academy community.
- 1.7 The academy'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 academy's use of CCTV and how it complies with the Act.
- 1.8 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 academy's data controller in their responsibilities as part of the requirements of this policy document, the academy'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 academy complies with 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 academy, including main staff/pupil and visitor entrances and academy 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 academy 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 should 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 civil rights and privacy are not violated. The academy 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 academy will make every effort to position cameras so that their coverage is restricted to the academy’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 academy 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 by the Headteacher / Principal or Director of the Trust.

6.2 A list of staff authorised to view images from this CCTV system will be held by the academy, and listed in appendix 1.

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 academy will respond to requests within 40 calendar days of receiving the written request and fee.
- 7.4 At the Director of the Trust's discretion, a fee of £10 may be charged per Subject Access Request.
- 7.5 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.

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 academy 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*. (*DELETE AS APPLICABLE)
- 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 academy should be directed to the Principal / Headteacher / Governing Body* in the first instance. (*DELETE AS APPLICABLE)
- 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 (e.g. adoption in UK of General Data Protection Regulation).

Appendix 1 – Checklist of Operation

The Academy'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 Academy 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 Name & Sign	Review Date
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
The name of the individual responsible for the operation of the system is:			
The reason for using CCTV has been clearly defined and installation / use of cameras is the best solution.			
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.			
Staff and members of the Academy community are consulted about the proposal to install and or continued use of CCTV equipment.			
Cameras have been sited so that they provide clear images and limit the opportunity to be tampered with.			
The potential impact on individuals' privacy has been identified and taken in to account in the use of the system.			
Cameras are located in the following areas:			

Cameras have been positioned to avoid intentionally capturing the images of persons not visiting the premises.			
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).			
Images from this CCTV system are securely stored in _____ and access is limited to the following authorised persons:			
Recorded images will be deleted after _____, unless they form part of an incident under investigation.			
Procedures are in place to respond to the police or individuals making requests for access to data held.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

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 Academy 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
- 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



Appendix 3 – IRIS Protocol (Issue 2)

IRIS Protocol – guidance for use of IRIS in Trust academies

Introduction

IRIS is a videoing facility based on individual user accounts which enables teachers and support staff to engage in self-observation, personal reflection, collaboration and coaching and remains under the control of the individual employee at all stages. It is possible to 'invite' either peers or members of senior staff to engage in a joint review of the lesson, and practitioners can choose to share with others more widely across the academy or Trust, thus aiding the development of practice.

IRIS adds another dimension to the development of teaching and learning, in-line with the co-operative values of self-help and self-responsibility. Through self-reflection, peer discussion and professional dialogue, the aim is to give teachers and other practitioners the opportunity to use IRIS as one part of a range of possible professional development tools. Because teachers can reflect on their own practice by seeing how they have taught, it enables learning discussions to be relevant and linked with real events within the classroom.

The IRIS system consists of videoing hardware which is placed in the classroom and switched on with the explicit permission of the user. The hardware is easy to use and uploads to a secure site where the practitioner can access their recordings to view at a later date. Recordings cannot be downloaded or saved outside of the IRIS system.

Whilst this document specifically covers the use of IRIS, there are a wide range of technologies available which can be used to support and enhance professional development; when considering their use, academies should ensure that the principles documented here are followed.

Protocol

1. Trust academies are encouraged to consider using IRIS as a tool to help develop quality of teaching and learning, but are not required to do so.
2. It is the responsibility of the Headteacher / Principal to ensure that parents are appropriately informed and relevant permissions for filming students / pupils are obtained. These permissions do not provide any rights to parents or pupils, whether or not they hold individual user accounts with IRIS, to access the films made. The school's "Home School Parent Agreement" should ideally have wording to the effect that video is used for professional development by employees at the school. Teachers should inform the class that IRIS is being used for the teachers' (or other employee's) professional development prior to the lesson starting.
3. Agreement should also be sought from any other persons present in the classroom at the time of filming, who should be informed that the camera is being used for the purpose of the user's personal development and training only and that it can record both video and audio.
4. As a learning community we recognise the need for teaching and learning development tools. Use of the IRIS system is voluntary, and no pressure will be placed on employees to use it, or to share their practice with other users if they have chosen to opt in.
5. Where IRIS is used, employees will be appropriately trained before being given access to the system.
6. IRIS will not be used as a tool linked to the performance management process; it should be considered as one of a range of methods available to use, in agreement with the member of staff, for professional development purposes only.

7. IRIS will not be used for surveillance purposes, or to monitor classroom delivery when the regular teacher is absent.
8. IRIS Connect have advised that legally, the ownership of the videos rests with the academy, who is ultimately responsible for the videos (data) as Data Controller under the terms of the Data Protection Act. However, the privacy rights of individual employees using IRIS is paramount to us, and they remain in full control of the films made from beginning to end of the process – but with the proviso that the film must not be shared more widely than with other employees of the Co-operative Academies Trust, unless additional permissions for its use are secured from the Headteacher/Principal. There must be no system 'override' put in place by academies to give administrator rights to remotely or subsequently view a lesson without the permission of the employee.
9. All individual users have the responsibility to protect their own data and the data of others, and not to disclose passwords, notwithstanding the responsibilities of the provider / data controller.
10. Employees may agree to share their videos with colleagues at their academy and/or between academies within the Trust. This can be arranged via IRIS who can create a "Co-operative Academies Trust" group which will allow teachers to share with each other. Where an employee decides to share, the system will be used confidentially, sensitively, with a focus on development, and with due respect for colleagues. They may recall the film from another user or group library at any time.
11. Films are stored in the IRIS system until such a time that the employee deletes the recording from the system. Employees may delete their films at any time. If leaving employment of the Trust, employees must delete all their films from the system.
12. Use of the IRIS system within an academy will be reviewed on an annual basis through consultation with all staff and local trade union representatives.