

Connect Academy Trust

CCTV Policy

Approved by the ELT of
Connect Academy Trust, September 2023

Amendments

Version	Date	Detail
1	9/9/17	Newly created policy
2	4/4/18	Amendments re GDPR and responsible person
3	12/03/2020	No changes
4	17/03/2022	No changes
5	Sept 23	No Changes
6	9/9/17	Newly created policy

Contents

1. Introduction
2. About the CCTV
3. Objectives
4. Statement of Intent
5. Operation of the System
6. Authorised Users – Roles and Responsibilities
7. Control of Cameras and Monitors
8. Recording Procedures
9. Breaches of this Policy
10. Monitoring
11. Complaints
12. Access by Data Subject
13. Public Information
14. Summary

Appendix 1 - Checklist for CCTV users

Appendix 2 - Register of CCTV Incidents and Reviews

CCTV Policy

1. Introduction

These guidelines are to assist Trust schools to remain within the law by regulating the management, operation and use of Closed Circuit Television (CCTV) systems within school grounds. It will assist you in setting out a Policy that will show best practice and maintain public confidence by demonstrating the school takes their responsibilities under The Data Protection Act 1998 (DPA), Freedom of Information Act 2000 (FOI), General Data Protection regulations(GDPR) and regulations by the Information Commissioners Office (ICO) seriously. It also covers the Codes of Practice, British Standards and Legislation impacting on the use of CCTV.

The ICO recently issued information which briefly mentioned CCTV. It highlighted the fact that an increasing number of schools use cameras for security. As recording and capturing of images of identifiable individuals involves the processing of personal information, it needs to be done in line with DPA principles. The school needs to inform staff, pupils and visitors why they are collecting personal information in the form of CCTV images (eg. security), this needs to be done via the privacy notice. The positioning of cameras, retention periods, why you keep images, who is allowed to access them and why, as well as subject access requests, all have to be considered.

2. About the CCTV

Trust schools have CCTV systems. The systems are whole school systems and are used to monitor outside spaces. These whole systems comprise a number of fixed external facing cameras located around the school sites. The system has a master monitoring location. The CCTV systems are wholly owned by the Trust and all cameras are monitored within each School, no external agency or organisation is involved in the monitoring process. This policy follows GDPR guidelines.

3. Objectives

The CCTV system is designed to assist in the protection of the building and contents as well as to increase the safety of all site users. The system should also deter crime and assist the Police in the detection, apprehending and prosecuting of any offenders. This will further assist in the protection of members of the public and private property.

4. Statement of intent

The Trust will treat the system and all information, documents and recordings obtained and used as data which is protected by GDPR. The cameras will be used to monitor activities on the school roofs, grounds and car park to identify and record any criminal activity against each school or its visitors. Authorised users must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained from the Person in Control (PIC), a record of the need for this action will then be kept by the PIC.

CCTV footage and associated knowledge will not be used for any purpose other than that mentioned in the objectives. Recordings will only be released to the media by written authority of the Police to assist in the investigation of a crime. Recordings will never be released for the purpose of entertainment. Warning signs, as required by the Code of Practice of the ICO, have been placed at all access routes around each school.

5. Operation of the System

The CCTV and system will be administered by the PIC in accordance with the principles and objectives of this policy. The PIC will delegate the daily management of the system to authorised members of staff. Authorised users will have defined roles and responsibilities (see below) with regard to the daily management and use of the system.

6. Authorised Members of Staff – Roles and Responsibilities (Data Controller/Manager)

The scheme will be managed by the PIC, in accordance with the principles and objectives expressed in this policy.

The day-to-day management will be the responsibility of each school Headteacher (PIC), SLT or Caretaker during the school day.

The control panel will only be used by the Headteacher, SLT or other staff as designated from time to time.

The CCTV system will be in operation 24 hours a day, every day of the year.

7. Control of Cameras and monitors

Anyone wishing to access the CCTV system or recordings must meet the requirements of the Data Controller and Data Managers. The authorised users must satisfy themselves of the identity of anyone wishing to access the CCTV

and the purpose of the access. Where any doubt exists permission will be refused.

In appropriate cases the emergency services may be called.

The IT team or other delegated person will ensure the whole system is working on a weekly basis and that the recording and cameras are functioning properly. Each school has a designated member of staff who is responsible for the administrative functions, including recordings and hard drive space, filing and maintaining all logs.

8. Recording Procedures

Any recordings taken from the hard drive must adhere to the following process to ensure they are suitable for any possible proceedings:

Transferred recordings must be uniquely identified (eg. date & time) and logged.

The disc or memory stick used for transfer must be clear of any other recordings.

Any recording required for evidential purposes must be sealed, witnessed, signed by the PIC, dated and stored in a separate, secure, evidence store. If a recording is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the PIC, dated and returned to the evidence store.

If the recording is archived the reference must be noted.

Under section 29 of the Data Protection Act 1998 the Police may request a viewing of recordings. Any viewings or recordings released to the Police or other authorised applicant will be logged on a register by the Data Manager.

Recordings released to the Police remain the property of the Trust and should be treated in accordance with this policy. The Trust also retains the right to refuse permission for the Police to pass to any other person the recording or any part of the information contained thereon. On occasions when a Court requires the release of an original recording this will be produced from the secure evidence store, complete in its sealed bag. If the Police ask the Trust to retain any copies they must be properly indexed and securely stored until required.

Applications from other bodies should be referred to the PIC. Satisfactory documentary evidence must be produced to release recordings if they are

required for legal proceedings or in response to a Court Order. People can make a request to view their footage by making a Subject Access Request in writing to the Trust.

9. Breaches of this Policy

Any breach of this policy by Trust staff will be initially investigated by the PIC, in order for them to take the appropriate disciplinary action. Any serious breach of this policy will be immediately investigated by an independent investigation carried out to make recommendations on how to remedy the breach.

10. Monitoring

Performance monitoring, including random operating checks, may be carried out by the PIC.

11. Complaints

Complaints about the Trust's CCTV system should be addressed to the PIC.

12. Access by the Data Subject

The Data Protection Act (GDPR) provides Data Subjects (individuals to whom 'personal data' relates) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made in writing to the PIC. (See section 8 for fees.)

13. Public Information

Copies of this policy will be available to the public on the school website or from the Trust office on request.

14. Summary of Key Points

- This policy will be reviewed every year by the PIC/ELT
- The CCTV system is owned and operated by each School
- The Control system is not open to visitors except by prior arrangement and with good reason
- Liaison meetings may be held with the Police and other bodies
- Any recordings will be used properly, indexed, stored and destroyed after appropriate use
- Recordings may only be viewed by authorised Trust staff and the Police
- Recordings required as evidence will be properly recorded, witnessed and packaged before copies are released to the Police

- Recordings will not be made available to the media for commercial or entertainment purposes
- Recordings will be disposed of securely
- Any breaches of this Code will be investigated by the PIC. An independent investigation will be carried out for serious breaches
- Breaches of the Code and remedies will be reported to the PIC.

15. References/Further information

Information Commissioners CCTV Code of Practice 2008

Criminal Justice and Public Order Act 1994

Criminal Procedures and Investigations Act 1996

Human Rights Act 1998

Crime and Disorder Act 1998

Data Protection Act 1998

Freedom of Information Act 2000

General Data Protection Regulations 2018

Regulation of Investigatory Powers Act 2000

Private Security Industry Act 2001

Protection of Freedoms Act 2012

Surveillance Camera Commissioners Code of Practice for Surveillance Camera Systems 2013 (forthcoming)

BSI British Standards - Alarm Systems - CCTV surveillance systems for use in security applications. BS EN 50132-7:1996

BSI British Standards - Closed Circuit Television - Management and Operation - Code of Practice. BS 7958:2009

APPENDIX 1 - CHECKLIST FOR USERS OF CCTV SYSTEMS

This CCTV system and the images produced by it are controlled by The PIC who is responsible for how the system is used and for notifying the commissioner about the CCTV system and its purpose (which is a legal requirement of the Data protection Act 1998).

Action	Date completed	Name/Signature	Review Date
There is a named individual who is responsible for the operation of the system.			
A system has been chosen which produces clear images.			
Cameras have been positioned to avoid 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 the responsible persons for the system contact details are displayed on the sign.			
Images from the CCTV are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light. (E.g. for a theft to have been noticed).			
Except for the police, images will not be provided to third parties,			
The organisation knows how to respond to individuals making requests for copies of their own images.			
Regular checks are carried out to make sure the system is			

working properly and produces high quality images.			
--	--	--	--

APPENDIX 2 - REGISTER OF CCTV INCIDENTS AND REVIEWS

Date Of Review	Data managers name & signature	Others Present at the viewing	Date & time of incident Reviewed	Details of actions taken