




Close Circuit Television (CCTV) Policy

Governor Committee Responsible:		Staff Lead(s):	Heather Willis
Status <i>(Statutory / Advisory)</i>	Non Statutory	Review Cycle	Annually
Last Review	September 2024	Next Review Date	September 2025
Chair of Governors	Daniel Gillingham Daniel Gillingham (chair@chcfederation.gloucs.sch.uk)		

Definitions	CCTV	Closed Circuit Television
	DVR	Digital Video Recorder
	ESD	Encrypted Storage Device used to pass on recorded images to a third party e.g. Police

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Finlay Community School.

1. Introduction

- 1.1 Finlay Community School uses closed circuit television (CCTV) images to reduce the threat of crime generally, protecting our premises and helping to ensure the safety of all of our staff, pupils and visitors consistent with respect for the individuals' privacy.
- 1.2 The system comprises of a number of fixed and dome cameras located both internally to cover reception, corridors, dining hall and externally to provide coverage of the gates, outside play facilities and car parks. The system does not have sound recording capability.
- 1.3 This policy takes account of all applicable legislation and guidance, including:-
- General Data Protection Regulations ("GDPR")
 - Data Protection Act 2018
 - CCTV Code of Practice produced by the Information Commissioner
 - Human Rights Act 1998
 - Surveillance Commissioner Code of Practice

2. Objectives

- 2.1 The objectives of the CCTV system are:-
- Increase personal safety of staff, pupils and visitors by providing a visual deterrent to potential offenders;
 - Obtain visual evidence of bullying, misbehaviour, vandalism and/or related incidents;
 - To protect the school building and its assets;
 - To support the Police in a bid to deter and detect crime;
 - To assist in identifying, apprehending and prosecuting offenders;
 - To protect members of the public and private property;
 - To assist in managing the school.

3. Statement of Intent

- 3.1 The school will treat the system and all information, documents and recordings obtained and used as data which is protected by the Data Protection Act.
- 3.2 Cameras will be used to monitor activities within the school and 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 wellbeing of the school, pupils, staff and visitors.

- 3.3 Static cameras will not focus on private homes, gardens and other areas of private property.
- 3.4 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals.
- 3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded images will only be released to the Police Designated Data Protection officer at the Local Authority.
- 3.6 The planning and design has endeavoured to ensure that the scheme will give 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.
- 3.7 Warning signs, as required by the Code of Practice issued by the Information Commissioner will be displayed at all access routes to areas covered by the school's CCTV.

4. Operation of the System

- 4.1 The System will be administered and managed by the Headteacher or delegated member of the leadership team and where appropriate a member of the administration team in accordance with the principles and objectives expressed in the policy.
- 4.2 The CCTV display monitor is held in the admin office where members of the Admin. Team monitor access and exit points from the school site. Access to other recorded images is restricted to the Headteacher and Senior Leadership Team.
- 4.3 The CCTV system will be operated 24 hours each day, every day of the year.
- 4.4 The Admin Team will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional. A weekly check that the date and time stamp recorded on the images is correct will also be carried out.
- 4.5 A regular maintenance programme is in place and maintenance will be carried out annually or as and when required.
- 4.6 Access to CCTV system monitors should be controlled and must not be viewed by unauthorised staff or visitors.

5. Image Storage Procedures

- 5.1 The medium on which we record images is digital.
- 5.2 In order to maintain and preserve the integrity of the images recorded from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
 - Copies may only be made by authorised personnel;
 - Each recording/image must be identified by a unique mark;
 - Before using, each recording medium (e.g.: USB Memory Stick) must be cleaned of any previous recording;
 - The requester must provide a USB drive for the footage
 - The Headteacher or nominated person shall register the date and time of the recording/image in the evidence log;

- Any recording/image required for evidential purposes must be sealed, witnessed, signed by the Headteacher, dated and stored in a separate, secure, evidence store. If this 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 Executive Headteacher, dated and returned to the evidence store;
 - If the recording/image is archived the reference must be noted;
 - Any data/recording/image must be archived securely for a period of not less than seven years.
- 5.3 Any recording/image may be viewed by the Police for the prevention and detection of crime and/or authorised officers of Gloucestershire County Council for supervisory purposes, authorised demonstration and training.
- 5.4 Any request to view or copy a recording/image must be made in writing where possible specifying (as far as possible) the date and time of the image(s). The school must contact the DPO officer at the Local Authority before providing a response to the request within 5 school days. If the decision is taken not to release the image(s), then they must be held and not destroyed until all legal avenues have been exhausted.
- 5.5 Viewing of ESD's by the Police must be recorded in writing. Requests by the Police can only be actioned under section 29 of the Data Protection Act.
- 5.6 Should images/recordings be required as evidence, a copy may be released to the Police under the procedures described above and will only be released to the Police on the clear understanding that it remains the property of the school, and that the recording/image and the information contained on it are to be treated in accordance with this Policy. The school retains the right to refuse permission for the Police to pass it to any other person. On occasions when a Court requires the release of the original recording/image and not a copy this will be produced from the secure evidence store, complete in its sealed bag.
- 5.7 The Police may require the school to retain the stored recording/image for possible use as evidence in the future. It must be properly indexed and properly and securely stored until it is needed by the Police.
- 5.8 Applications received from outside bodies (e.g. solicitors) to view or release tapes will be referred to the Headteacher, in all circumstances the Headteacher must take advice from the DPO. In these circumstances the recording/image will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.
- 5.9 In normal circumstances images will be deleted and overwritten every calendar month.

6. Siting the Cameras

- 6.1 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 School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.
- 6.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises.
- 6.3 CCTV will not be used in classrooms.

6.4 Members of staff should have access to details of where CCTV cameras are situated. The exception stated in the Code of Practice is if cameras are placed for the purpose of covert monitoring (see below).

7. Covert Monitoring

7.1 The school may in exceptional circumstances set up covert monitoring. For example:

- i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
- ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

7.2 In these circumstances authorisation must be obtained from the Chair of Governors

7.3 Covert monitoring must cease following completion of an investigation.

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

7.5 Images captured on the DVR should not be used for the purpose of Performance Management or Assessment.

8. Digital Video Recorder

8.1 A Digital Video Recorder (DVR): A device used to record and store video footage.

8.2 All staff members who have access to DVRs must familiarise themselves with this policy and adhere to its guidelines. They are responsible for ensuring the appropriate use of DVRs and protecting the privacy of individuals.

8.3 Parents and guardians should be informed about the school's policy on DVRs and their rights regarding their child's personal data.

A digital video recorder will be used in school, for exceptional purposes only. In such circumstances prior written consent will be obtained from individuals before capturing their personal data using DVRs, except in cases where the use of DVRs is necessary for the safety and security of individuals or the school premises.

In these exceptional circumstances, footage will be retained for as long as is deemed necessary for legitimate educational purposes. After the retention period, the footage will be securely deleted or destroyed. The footage will be stored securely, by our data controller.

9. Breaches of the Policy (including breaches of security)

9.1 Any breach of the Policy by school staff will be initially investigated by the Headteacher, in order for he/she to take appropriate disciplinary action. Misuse of CCTV images could be a criminal offence.

9.2 Any serious breach of the Policy/Commissioner's Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10 Storage and Retention of CCTV images

10.1 Recorded data will not be retained for longer than is necessary, (up to a maximum of one calendar month). 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.

10.2 All retained data will be stored securely on the network with restricted access.

11 Access to CCTV images

11.1 Access to recorded images will be restricted to those staff authorised to view them (see 4.2), and will not be made more widely available

12 Subject Access Requests (SAR)

12.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

12.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

12.3 The school will respond to requests within 30 calendar days of receiving the written request and fee.

12.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

13 Access to and Disclosure of Images to Third Parties

13.1 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 school where these would reasonably need access to the data (e.g. investigators).

13.2 Requests should be made in writing to the Headteacher.

13.3 The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

14 Complaints

14.1 Complaints and enquiries about the operation of CCTV within the school should be made in accordance with our school's complaint policy.

15 Public Information

15.1 Copies of this Policy will be available to the public via the website or school office when requested.

16 Appendices

See below



Finlay Community School

**Record of Request of Access to CCTV Images
Third Party Viewing (i.e. Police, Local Authority etc.)**

Date and time of viewing:

Date: Time:

Names of persons viewing the CCTV image:

Name	Designation
.....
.....
.....
.....

Reason for viewing the CCTV images:

.....
.....
.....

Outcome, if any, of the viewing:

.....
.....
.....

Crime incident Number (if applicable):

Date and time copy created for evidential purposes:

Reference No: Date: Time:

Signature of Person Authorised to Collect the Medium:



Finlay Community School

Name:

Address:

.....

.....

.....

Telephone:

Reason for Request:

.....

.....

.....

Date Image Recorded:

Time Image Recorded:

Location:

Signed: *Date:*