



CCTV Policy

Date of issue:	April 2024
Responsible Sub-Committee:	Finance & Resources
Linked Policies:	Child Protection & Safeguarding Policy Data Protection Policy Subject Access Policy Data Breach Policy Data Retention Policy Privacy Notices Freedom of Information Policy Police Request Procedure Court Request Procedure
Review Date:	April 2027
Target Audience:	All Staff
Dissemination Via:	SharePoint

Version	Section	Amendments	Date	Author
2.0		The existing policy has been recreated to include all current legislation. The sections from the old policy have been added to this policy. All schools have adequate CCTV signs installed as required.	April 2024	IT Director

		CCTV footage that is exported now has a retention of 30 days All CCTV footage needs to be stored securely. Maintenance providers have been removed as not required. Schools have this information. The roles that could have access to CCTV footage have been added.		
8.2.	8.2	Section updated to refer to SAR policy		

Contents

1. Aims.....	3
2. Relevant legislation and guidance.	3
3. Location of the cameras.....	4
4. Roles and responsibilities.....	4
5. Operation of the CCTV system.....	5
6. Storage and retention of CCTV footage.....	6
7. Redaction of CCTV.....	6
8. Access to CCTV footage.....	6
9. Data protection impact assessment (DPIA).....	8
10. Security	8
11. Monitoring	8

1. Aims

This policy sets out our approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems.

1.1 Statement of Intent

The purpose of the CCTV system (video and/or audio) is to:

- Make members of our community feel safe
- Protect members of our community from harm to themselves or to their property
- Deter criminality
- Protect Trust assets and buildings
- Assist police to deter and detect crime
- Assist the courts
- Determine the cause of accidents / incidents
- Assist in the effective resolution of HR cases / Allegations/ H&S incidents / Insurance claims / behavior incidents/ complaints grievance proceedings
- To assist in the defense of any litigation proceedings
- Follow individuals, unless it falls into the purposes set out above.

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

Footage/any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime/alleged crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant Legislation and Guidance

2.1 Legislation

[UK General Data Protection Regulation](#)

[Data Protection Act 2018](#)

[Human Rights Act 1998](#)

[European Convention on Human Rights](#)

[The Regulation of Investigatory Powers Act 2000](#)

[The Protection of Freedoms Act 2012](#)

[The Freedom of Information Act 2000](#)

[The Education \(Pupil Information\) \(England\) Regulations 2005 \(as amended in 2016\)](#)

[The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#)

[The School Standards and Framework Act 1998](#)

[The Children Act 1989](#)

[The Children Act 2004](#)

[The Equality Act 2010](#)

2.2 Guidance

[Surveillance Camera Code of Practice \(2021\)](#)

3. Location of the Cameras

Cameras are located in places that require monitoring in order to achieve the aims of this policy and where the school has identified a need and where CCTV is the most effective solution.

Cameras will not be used in areas where the subject has a heightened expectation of privacy e.g., changing rooms or toilet cubicles. Where there are cameras in the communal area of the toilets, these will not point towards the inside of toilet cubicles or urinals. In these areas, the school will use increased signage in order that those under surveillance are fully aware of its use.

Signage is in place to advise where CCTV cameras are situated. This sign identifies the Trust as the operator of the CCTV system and as data controller.

Cameras are not aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

In addition, for schools which are managed by PFI providers the PFI company have their own CCTV cameras located for site security purposes.

4. Roles and Responsibilities

4.1 Trustees

To approve the CCTV policy.

4.2 The Headteacher

The Headteacher has responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

The Headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Ensure that all staff comply with this policy
- Approve any expansion or upgrading to the CCTV system, after having taken advice from the IT Director and considered the result of a data protection impact assessment
- Decide, in consultation with the data protection officer (DPO), whether to comply with disclosure of footage requests from third parties. Disclosure of footage must follow UK Law (GDPR)

4.3 The IT Director

The IT Director will:

- Liaise with the DPO to ensure that the use of the CCTV system is in accordance with this policy
- Review the CCTV policy to check that the trust is compliant with relevant legislation

- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the IT Team in the use of the system and in data protection
- Ensure footage is destroyed when it falls out of the retention period
- Authorise access to and keep a log of persons that have access to CCTV footage and review termly
- Review the CCTV footage access log termly

4.4 The Data Protection Officer (DPO)

The data protection officer (DPO) will:

- Advise on updates to this policy in line with legislation and data protection updates
- Ensure footage is obtained in a legal, fair, and transparent manner
- Ensure Trust privacy notices include the use of CCTV recordings
- Receive and consider requests for third-party access to CCTV footage

4.5 The IT Team

The IT Team will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the date and time stamps are accurate termly
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure CCTV systems do not infringe on any individual's reasonable right to privacy in public spaces
- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period

4.6 Staff

All staff using CCTV will:

- Have completed CCTV training in advance
- Comply with this policy
- Only access CCTV for specific cases or incidents being investigated with prior approval from the Headteacher

4.7 PFI

PFI providers are responsible for the maintenance and data security of their own cameras.

5. Operation of the CCTV System

The CCTV system will be operational 24 hours a day, 365 days a year and will record video and may record audio where available as a precaution to protect all.

The Trust is registered with the Information Commissioner's Office - ZA348223.

Recordings will have date and time stamps. This will be checked by the IT Team termly and when the clocks change.

6. Storage and Retention of CCTV Footage

6.1 Storage of Main CCTV System

Footage will be retained for 30 days in line with the retention policy locally on school servers or in the Cisco Meraki cloud. At the end of the retention period, the files will be overwritten automatically by the CCTV system.

6.2 Storage of CCTV Extracts for Incidents or Cases

On occasion footage (or stills of footage) may be retained for longer than 30 days, for example where we or a law enforcement body is investigating a crime or if an H&S, HR, or Safeguarding incident has been identified, to give opportunity to view the images as part of an active investigation.

In these cases, recordings will be downloaded and stored in the associated investigation file (H&S, Safeguarding, HR) securely in restricted folders on SharePoint called CCTV Exports, so that the data will be secure, and its integrity maintained, so that it can be used as evidence if required. Retention of this footage will be in line with the case it relates to as set out in the Data Retention Policy (i.e. safeguarding data, H&S, HR).

Access to these folders will only be by authorised staff for the incident e.g. H&S, Safeguarding, Grievance, Behaviour, Complaint, Disciplinary cases.

CCTV will not be stored in any other location or file.

6.3 Deletion of CCTV Footage

The IT Director will carry out annual checks to determine whether footage is being stored accurately and being deleted in line with the Retention Policy.

7. Redaction of CCTV

If CCTV footage contains sensitive content, such as footage of a sexual nature, it will be automatically deleted from the system after being exported, if necessary. The exported file will be stored in a secure location with restricted authorised access. This measure ensures that the content cannot be viewed by individuals who have access to CCTV footage.

8. Access to CCTV Footage

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log - [GDPR - CCTV Access Log - All Documents \(sharepoint.com\)](#)

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

Access will be restricted to those who have been identified as having a need to have access to CCTV footage, for certain recordings, where there are exceptional circumstances, such as sexual content or in the event of a court case.

8.1 Staff Access

The following members of staff may have authorisation to access the CCTV footage as approved by the Headteacher or C-Suite, the Headteacher will also have access:

- Senior Leadership Team
- C-Suite and DPO
- Behaviour Team
- Pastoral Team
- Safeguarding Team
- IT Teams
- Facilities Team
- Admin Staff

CCTV systems are only accessible via a secure login and individual password which is unique to each staff member.

- Investigation lead for cases which involve the use of CCTV evidence may require access. In these cases, authorisation will be given by the Headteacher (e.g. for H&S, Safeguarding, Grievance, Behaviour, Complaint, Disciplinary cases).

C-Suite may need access where required for review of incidents.

PFI providers may be shown CCTV footage from the Trust cameras, but they will not be granted access to the system or have unsupervised viewing rights.

The Data Protection Officer may need access where required to comply with Data Protection Policies – i.e. Subject Access Requests, Court, or Police Requests.

CCTV footage will only be accessed from Trust devices and only on a secure network.

All staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the CCTV system may be committing a criminal offence and may face disciplinary action.

It is the responsibility of the Headteacher and IT Director to delete footage in line with the retention policy set for the case.

8.2 Subject Access Requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves. If requests are received the Trust will follow the Subject Access Policy (SAR). When making a request, individuals should provide the school with reasonable information such as the date, time, and location the footage was taken to aid trust staff in locating the footage.

There are circumstances where information (including CCTV footage and images) requested in a subject access request can be withheld, these are set out in our Subject Access Policy.

8.3 Third-Party Access

CCTV footage will only be shared with a third party on receipt of a valid request for data (such as a police/court/safeguarding case). See the details of our Court and Police Request Policy.

All requests for access should be set out in writing and sent to the Headteacher / Designated Safeguarding Lead / Business Manager and the DPO.

The DPO will consider very carefully how much footage to disclose and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

9. Data Protection Impact Assessment (DPIA)

When the CCTV system is replaced, developed, or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary, and proportionate.

Those whose privacy is most likely to be affected, including the Trust community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be reviewed annually and whenever cameras are moved, and new cameras are installed.

If any security risks are identified during the DPIA, the school will address them as soon as possible.

10. Security

The IT Team will be responsible for overseeing the security of the CCTV system and footage.

The system will be checked for faults once a term.

Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure.

Footage will be stored securely and encrypted.

The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use.

Proper cyber security measures will be put in place to protect the footage from cyber-attacks.

Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied, and tested as soon as possible.

11. Monitoring

The policy will be reviewed every 3 years by the DPO and IT Director to consider whether the continued use of a CCTV cameras remains necessary, proportionate, and effective in meeting its stated purposes.