St Christopher's the Hall School

CCTV Policy

Policy Owner: Chief Operating Officer (COO)

ISSR Reference: N/A

Interim Review: Trinity 2025

Approved: Full Governing Body Michaelmas 2024

Next Review: Michaelmas 2025

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Annual review	Chief Operating Officer	Trinity 2025	New policy

Contents

1. Introduction and aims

This policy is applicable to staff, pupils, parents/carers and visitors to St. Christopher's the Hall School (the school) and aims to ensure all parties are clear on the rationale for and management of CCTV at the school.

The school recognises that CCTV systems can be privacy intrusive. This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on the school's property. The school has completed a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below. The result of the data protection impact assessment has informed the school's use of CCTV and the contents of this policy.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

2. Legislation & definitions

2.1 Legislation

This policy is based on advice from Judicium Education, and informed by the following legislation:

- UK General Data Protection Regulation (UKGDPR), 2018
- Data Protection Act, 2018
- Regulation of Investigatory Powers Act (RIPA)
- Privacy and Electronic Communications Regulations (PECR)
- Human Rights Act 1988

2.2 Definitions

CCTV	Close circuit television video cameras used for surveillance
Surveillance	The act of watching a person, or a place
Covert surveillance	The operating of cameras in a place where people have not been made aware that they are under surveillance
Subject Access Request (SAR)	A request made by an individual to access their personal information that is held by an organisation.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

St Dunstan's Education Group's (the Group) governing board has ultimate responsibility for data protection, which includes ensuring that CCTV is operated within the parameters of this policy but will delegate day-to-day responsibility to the Chief Executive Officer of St Dunstan's Education Group. The governing body has a duty to:

- Ensure an approved CCTV Policy is in place and reviewed annually
- Monitor the application of the CCTV Policy.

3.2 The Chief Executive Officer of St Dunstan's Education Group

The Chief Executive Officer of St Dunstan's Education Group (CEO) is responsible for:

- Day-to-day management of all data protection matters, including management of CCTV, in accordance with this policy
- Delegating responsibilities to other competent members of staff.

3.3 Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Taking responsibility for all day-to-day leadership and management of the CCTV system
- Liaising with the Data Protection Officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated objectives and that its use is needed and justified
- Ensuring that the guidance set out in this policy is followed by all staff
- Ensuring that all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and data protection
- Ensuring that the CCTV system is not infringing on an individual's reasonable right to privacy in public spaces
- Ensuring that footage is destroyed when it falls out the retention period
- Receiving and considering requests for third-party access to CCTV footage
- Signing off any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taking into account the result of the data protection impact assessment
- Deciding, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties
- Ensuring that the CCTV policy is reviewed at least annually.

3.4 Data Protection Officer (DPO)

The DPO, Judicium Education, is responsible for:

- Monitoring compliance with data protection law and developing related policies and procedures, including the CCTV policy
- Conducting an annual audit of each individual school's data protection procedures, including management of CCTV
- Advising on, and assisting the Group and individual schools with, carrying out data protection impact assessments
- Ensuring footage is retained in a legal, fair and transparent manner.

3.5 The System Manager

The school's Systems Manager is the Site Manager. They are responsible for:

- Overseeing the day-to-day maintenance and operation of the CCTV system
- Overseeing the security of the CCTV system and footage
- Checking the system for faults and security flaws termly
- Checking that data and time stamps are accurate termly
- Ensuring that CCTV systems are working properly, and that the footage is of high quality so that individuals pictured in the footage can be identified
- Carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period.

3.6 Staff

All staff are responsible for:

- Using CCTV in accordance with this policy
- Completing data protection and cybersecurity training
- Seeking advice from the COO if they have concerns that this policy is not being followed correctly.

3.7 Pupils and parents/carers

All pupils and parents/carers are responsible for:

- Understanding that CCTV is used within the car park and the purposes of the system
- Seeking advice from the COO if they have any concerns that this policy is not being followed.

4. Purpose of the CCTV system

The school's CCTV system is registered with the Information Commissioner's Office under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Action 2018 and UK GDPR.

The purpose of the CCTV system is to:

- Protect pupils, staff and visitors against harm to their person and /or property
- To increase a sense of personal safety and reduce the fear of crime
- To encourage all members of the school community to adhere to the school rules and to assist us in identifying and sanctioning those who may have breached these rules; evidence from CCTV will be taken into account when determining sanctions, where appropriate
- To allow us to locate members of the community
- Deter criminality in the school
- Protect the school's assets and buildings
- Assist the police to deter and detect crime
- Assist in identifying, apprehending, and prosecuting offenders
- Assist in establishing the cause of accidents and other adverse incidents to prevent recurrence
- Assist in the effective resolution of any disputes which may arise in the course of pupil or staff disciplinary and grievance proceedings
- Assist in managing the school
- To assist in the defence of any litigation proceedings.

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor individuals in spaces where they have a heightened expectation of privacy, for example, toilets and changing rooms
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated in the objectives above.

Footage or information gleaned through the CCTV system will never be used for commercial purpose. 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.

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If a situation arises where covert surveillance is needed, the proper authorisation forms from the Home Office will be completed and retained.

5. Operation of the CCTV system

5.1 Operating times

The CCTV system is operational 24 hours a day, 365 days a year. Recordings will have a date and time stamp. This will be checked by the Systems Manager termly and when the clocks change.

5.2 Security of the CCTV system

The System Manager is 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 wherever possible. Any camera operation equipment will be securely locked away when not in use

Full cyber security measures will be put in place to protect the footage from cyberattacks. These measures are detailed in the Group's Information Security Policy.

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

5.3 Storage of CCTV footage

Footage will be retained for a **maximum** of 5 days on the network video recorders. At the end of the retention period, the files will be overwritten automatically.

The system does not have the ability to download images. If required, screenshots will be taken of an incident and stored within the school's cloud storage solution and shared only with the relevant parties.

The Systems Manager will carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period.

5.4 Data Protection Impact Assessment (DPIA)

The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including replacement, development and upgrading.

The system is used only for the purpose of fulfilling the objectives stated in Section 4.

When the CCTV system is replaced, developed or upgraded, a DPIA will be carried out to ensure the objective of the system is still justifiable, necessary and proportionate. The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the School Operations Manager and the COO.

Those whose privacy is most likely to be affected, including the school's community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place. A new DPIA will be completed annually and/or whenever cameras are moved, and/or new cameras are installed.

5.5 Access to CCTV footage

Access to CCTV footage will only be given to authorised persons for the purpose of pursuing the objectives set out in Section 4, or if there is a lawful reason to access the footage. The staff member authorising access, normally the CEO, COO, Head of the school, or the School Operations Manager, must be satisfied of the identify and legitimacy of the purpose of any person making such request. Where any doubt exists, access will be refused until legal advice is sought. Any footage access will be logged in a CCTV Access Log: recording name, date and time, details of images viewed and the reason for accessing.

CCTV footage will only be accessed from authorised work devices, or from visual display monitors. Any visual display monitors will be positioned so that only authorised personnel will be able to see the footage. Any member of staff who misuses the surveillance system may be committing a criminal offence and may face criminal investigation, as well as internal disciplinary proceedings.

5.6 Staff access to CCTV footage

The following members of staff have authorisation to access the CCTV footage:

- The Chief Executive Officer
- Chief Operating Officer
- The Head of the school
- The School Operations Manager
- The Site Manager
- Director of Estates and Commercial Activities

- Anyone with express written permission of the CEO or COO.

5.7 Subject Access Requests

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves. This would be considered a Subject Access Request (SAR).

Upon receiving the request, the school will immediately issue a receipt and will then respond within one calendar month. All staff are trained to recognise SARs. When a SAR is received staff should inform the COO in writing. 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 staff in locating the footage. On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the data subject would prejudice an ongoing investigation.

Prior to releasing footage, images that may identify other individuals will be obscured to prevent unwarranted identification, or parts of the footage redacted. If this is not possible, the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it. This disclosure will happen in one of three ways:

- The subject could be invited in to see the footage under supervision; or
- The footage contains no data other than that of the subject, which means no special processing is required and can be forwarded directly to the subject; or
- The footage contains other's data, which may require redaction.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

The Group's Data Protection Policy details data subject's rights, the process of making a request, and what to do if a data subject is dissatisfied with the response to the request.

5.8 Third-party requests

CCTV footage will only be shared with a third-party to further the objectives of the CCTV system set out in Section 4.

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage, e.g. investigators.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, seeking 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 COO in consultation with the DPO.

5.9 Downloading captured data on to other media

In order to maintain and preserve the integrity of the data and to ensure their admissibility in any legal proceedings, any downloaded media or screenshots used to record events from the hard drive will be prepared in accordance with the following procedures:

- Each downloaded media /screenshots must be identified by a unique mark
- Before use, each downloaded media must be cleaned of any previous recording
- The System Manager will register the date and time of downloaded media insertion / screenshot, including its reference
- Downloaded media / screenshots required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media 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 and signed by the System Manager, then dated and returned to the evidence store
- If downloaded media is archived, the reference must be noted
- If downloaded media is put onto a device, the device will be encrypted and password protected.

5.10 Release of footage to the police

Images may be viewed by the police for the prevention and detection of crime and by those identified in 5.3. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it is preferable for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school and downloaded media (and any images contained thereon) are to be treated in accordance with data protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when

a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

6. Locations of cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in Section 4). Cameras are positioned to maximise coverage, but there is no guarantee that all incidents will be captured on camera. CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc. Cameras are not, and will not, be aimed off school grounds into public spaces or private property.

Wherever cameras are installed appropriate signage is in place to warn members of the community that they are under surveillance. All CCTV signage will:

- Identify the school as the operator of the CCTV system
- Identify the school as the data controller
- Provide contact details for the school.

Appendix A details all camera locations.

7. Complaints

Complaints regarding this policy should be directed to the COO and made in accordance with the Group's Complaints Policy.

8. Monitoring

This policy will be reviewed by the COO annually. At every review, the policy will be approved by the Finance and Resources Committee.

9. Links with other policies and documents

This CCTV Policy links to the following Group policies and documents:

- Data Protection Policy [Group]
- Data Breach Policy [Group]
- Data Retention Policy[Group]
- Information Security Policy [Group]
- Privacy notices [Group]

Appendix A: Camera locations

Type	Location	Audio	Capacity	Fixed/PTZ	Sample Image
Bullet/Dome	Car Park	No	As NVR	Fixed