



St Hilary's Prep School Policy

CCTV Policy

Introduction

We actively promote democracy, the rule of the law, individual liberty and mutual respect of those with different faiths and beliefs. These are fundamental British Values which underpin all that we offer, as does our School Motto 'Not for oneself but for all.'

1. Aims

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 school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

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

CCTV footage will only be processed for the purposes identified in this policy and the School's applicable privacy notice. Any proposed new purpose will be assessed by the DPO before implementation, including consideration of compatibility, lawful basis, necessity and proportionality, and whether the DPIA and privacy information require updating.

The School is the data controller for personal data processed through its CCTV system and is registered with the Information Commissioner's Office (ICO). The system will be operated in accordance with the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

Footage or 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.

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.

1.2 Lawful basis and data protection principles

The School will identify and document an appropriate lawful basis for each CCTV processing activity. For the School's routine CCTV use, legitimate interests may be relied upon where appropriate and a Legitimate Interests Assessment (LIA) will be completed and kept under review. Consent will not be relied upon as the lawful basis for routine CCTV surveillance. CCTV will be used only where necessary and proportionate, with regard to the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

2. Relevant legislation and guidance

This policy is based on:

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. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

4. Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

5. Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

- Pedestrian Gate – looking out towards the entrance steps
- Above the Pedestrian Gate – looking down the main driveway

- Art Room – looking towards the main building entrance
- Art Room – looking towards the Drop Off Zone in the car park
- Art Room – looking towards the entrance steps and car park
- Main front door
- Outside wall of Year 2 classrooms – looking down the main driveway
- Outside wall of Year 1R classroom – looking towards the Music Room entrance
- Outside wall of Pepper pot dining hall – looking towards picnic benches and Top Lawn
- Outside wall of side entrance – looking towards Courtyard gate
- Outside wall of Music room – looking towards boundary and Music room fire exit
- Outside wall of Music room – looking towards boundary (other direction)
- Outside Hall wall – looking towards boundary and Kindergarten mud kitchen play area
- Medical Room – this camera does not record and is for monitoring only

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

5.1 Transparency, signage and privacy information

Clearly visible signs will be displayed at appropriate entrances and locations to inform pupils, staff, parents, visitors and other individuals that CCTV is in operation, the purpose of the surveillance and how to contact the School about the processing. The School's privacy notices will explain its CCTV use, lawful basis, retention period, sharing arrangements and individuals' rights. Where new CCTV is installed or materially changed, the School will consult pupils, parents/carers and staff as appropriate and explain where cameras will be located and how footage will be used.

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

6. Roles and responsibilities

6.1 The governing board

The governing board has the ultimate 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.

6.2 The Headmaster

The Headmaster will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure 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 in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

6.3 The data protection officer

The data protection officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments

- Act as a point of contact for communications from the Information Commissioner's Office
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- 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 that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

6.4 The system manager

The system manager will:

- 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
- Ensure the data and time stamps are accurate

7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system will not record audio.

Any audio-recording capability provided by the system will be switched off by default. The School does not use live facial recognition through its CCTV system. Facial recognition, biometric identification, behavioural analytics or similar functionality will be disabled by default and will not be activated without a separate legal, safeguarding and data-protection assessment, including a DPIA and identification of any additional lawful conditions required for biometric or other special-category data.

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

8. Storage of CCTV footage

Footage will normally be retained for 30 days. The School has selected this period as a proportionate period for its stated security and safeguarding purposes and will review it periodically. At the end of the retention period, files will be overwritten or securely deleted automatically unless there is a lawful and documented reason to retain particular footage for longer.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation. Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

Footage is stored on the hard drive of the recording system. This is stored in the Main Office of the School, which is locked and the area alarmed when the School is closed.

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

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

9.1 Staff access

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

- The Headmaster: Mr Duncan Sinclair
- The Data Protection Officer: Mrs Hannah Wynn (Business Manager)
- The System Manager: Mr Scott Mansell (ICT Manager)
- The Site Manager: Mr Dimi Aristidov
- Anyone with express permission of the Headmaster

CCTV footage will only be accessed from authorised devices, or from the visual display monitors.

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

Authorised access rights will be reviewed regularly and will be removed promptly when a member of staff changes role, leaves the School or no longer requires access. Access will be limited to the minimum necessary for the individual's role.

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

9.2 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.

Upon receiving a valid request, the School will acknowledge it and respond without undue delay and in any event within one calendar month, subject only to any lawful extension permitted by data protection legislation. School holidays do not, of themselves, extend this deadline.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO 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 school 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 subject would prejudice an ongoing investigation.

Where footage contains personal data relating to other identifiable individuals, the School will consider whether that information can reasonably be redacted or obscured and whether disclosure is otherwise lawful. The School will balance the requester's right of access against the rights and freedoms of third parties in accordance with data protection legislation.

Consent from a third party may be considered where appropriate, but is not the only factor in deciding whether disclosure is lawful. The School will not disclose third-party personal data merely by converting footage into still images unless the relevant data-protection requirements are satisfied.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

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.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the [ICO website](#).

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

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).

All requests for access should be set out in writing and sent to the Headmaster and the DPO.

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, 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.

10. 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 its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

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.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by Mrs Hannah Wynn.

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

The DPIA will be reviewed at least annually and whenever there is a material change to the CCTV processing, including the installation or relocation of cameras, a material change to field of view, a new monitoring purpose, remote or cloud access, AI or analytics functionality, facial-recognition capability, audio capability, or a significant software or system upgrade. Where a change is likely to result in high risk, it will not be implemented until the risks have been assessed and appropriate safeguards put in place.

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

11. Security

- The System Manager 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 wherever possible
- 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 as soon as possible

12. Complaints

General complaints about the operation of CCTV should be directed to the Headmaster or DPO in accordance with the School's complaints policy. Complaints concerning the processing of personal data will be handled through the School's data-protection complaints procedure. Individuals will be informed of their right to raise a concern with the Information Commissioner's Office where applicable.

13. Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14. Links to other policies

- Privacy Notice and Data Protection Policy
- Biometric data policy
- Safeguarding Child Protection policy

Created: January 2024, June 2024, July 2025; updated September 2026

Next review date: September 2027

Person responsible: Mrs Hannah Wynn (Business Manager), Scott Mansell (IT Manager)