



# CLOSED CIRCUIT TELEVISION (CCTV) POLICY

## Table of Contents

1.	Aims.....	2
1.1	<i>Statement of intent</i> .....	2
2.	Relevant legislation and guidance .....	2
3.	Definitions .....	3
4.	Covert surveillance .....	3
5.	Location of the cameras .....	3
6.	Roles and responsibilities .....	3
6.1	<i>The governing body</i> .....	3
6.2	<i>The Principal</i> .....	3
6.3	<i>The Data Protection Officer</i> .....	4
6.4	<i>The Technical Director</i> .....	4
6.5	<i>CCTV Operators</i> .....	4
7.	Operation of the CCTV system.....	4
8.	Storage of CCTV footage.....	5
9.	Access to CCTV footage .....	5
9.1	<i>Staff access</i> .....	5
9.2	<i>Subject access requests (SAR)</i> .....	5
9.3	<i>Third-party access</i> .....	6
10.	Data protection impact assessment (DPIA) .....	6
11.	Security.....	6
12.	Complaints.....	7
13.	Monitoring.....	7
14.	Related policies.....	7

**Reviewed by:**

O Hickmott – Technical  
Director

**Date:** 20/06/2022

**Last reviewed on:**

June 2022

**Next review due by:**

June 2023

**Ratification by Governors on:**

July 2023

## 1. AIMS

Herne Bay High School makes use of surveillance and closed-circuit television (CCTV) to maintain a safe and secure environment for staff, students, visitors and to protect school property and assets. 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.

Notification of the use of CCTV at Herne Bay High School is disclosed within the Information Commissioner's Office register entry Z923423X.

### 1.1 STATEMENT OF INTENT

The purpose of the CCTV system is to:

- Ensure 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)
- Pursue any other purposes than the ones stated above

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

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

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.

## 2. RELEVANT LEGISLATION AND GUIDANCE

This policy refers to, and complies with, the following legislation and guidance:

- 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

- Communications Act 2003
- Keeping Children Safe in Education 2022
- Education and Inspections Act 2006
- 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, the proper authorisation forms from the Home Office will be completed and retained.

### 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).

The school will make every effort to position cameras to only cover school premises. Where camera siting may include views of private residence or public property, image obscuring measures will be enabled within the camera software.

All cameras installed will be 'static' with fixed focal length and no ability to pan or tilt.

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

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

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

Camera locations will be graphically represented on a CCTV Camera Locations guide that will be available for review by school staff upon request.

### 6. ROLES AND RESPONSIBILITIES

#### 6.1 THE GOVERNING BODY

The governing body 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 PRINCIPAL

The Principal will:

- 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 termly 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 TECHNICAL DIRECTOR

The Technical Director 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
- 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 data and time stamps are accurate termly

### 6.5 CCTV OPERATORS

All CCTV operators will:

- Abide by this policy in the use of the CCTV system and footage
- Protect against unauthorised access to the CCTV system and footage
- Report potential faults and security flaws

## 7. OPERATION OF THE CCTV SYSTEM

- The CCTV system will be operational 24 hours a day, 365 days a year.
- The system is registered with the Information Commissioner's Office register entry Z923423X.
- The system will not record audio.
- 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 be retained for 31 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 31 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.

CCTV storage will be resilient and have redundancy to ensure the integrity of the data.

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.

The DPO will carry out regular 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 individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

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

### 9.1 STAFF ACCESS

Access to the CCTV system and recorded images will be provided by the school's Technical Director at the discretion of the Principal. Staff with permission to access the system will have their details logged within the CCTV Access Log.

This log is to detail:

- Full name of user
- Position held within school
- Purpose of access
- Level of access provided
- Date of access provided

Every effort will be taken to ensure no unauthorised person views the images. The system will never be left unattended and only be accessed for the indented purpose.

CCTV footage will only be accessed from authorised personnel's work 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.

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 DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request the school will immediately issue a receipt and will then respond within 30 days.

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.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming static images may be released instead.

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 Principal 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 Principal or DPO are the only members of the school community who can authorize disclosure of information to any of the aforementioned. All requests for disclosure must be via a disclosure request form and will be recorded in the CCTV disclosure log, where requests for disclosure are made by law enforcement a STORM number must be requested and recorded in the disclosure log. All disclosures will be recorded by the DPO.

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

## 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 the 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.

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.

A new DPIA will be completed when new cameras are installed or the system is expanded.

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

## 11. SECURITY

- The Technical Director 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
- Proportionate cyber security measures will be put in place to protect the footage from cyber attacks
- The system will be segregated from the school's internet connection to ensure it is not accessible remotely, unless via secured Virtual Private Network connection.
- 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

Complaints should be directed to the headteacher or the DPO and should be made according to the school's complaints policy.

## 13. MONITORING

The Principal and Technical Director monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually and ratified by the school Governing Body.

## 14. RELATED POLICIES

This policy should be read alongside the school's policies on:

- Data protection
- Privacy notices for parents, pupils, staff, governors and suppliers
- Staff discipline
- Behaviour
- Safeguarding and child protection