



**Crompton Primary School**

## **CCTV Policy**

<b>Date written</b>	June 2025
<b>Date of review</b>	September 2026
<b>Headteacher</b>	Mrs G Croston
<b>Chair of Governors</b>	Mrs L Dowd

## **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.

## **Statement of intent**

Having CCTV in a primary school serves as a proactive measure to ensure the safety and security of pupils, staff, and visitors. By providing continuous monitoring of school premises, CCTV cameras act as a deterrent to potential threats such as vandalism, theft, or unauthorised entry. Additionally, they enable quick response to emergencies, help in investigating incidents, and provide accountability in case of disputes. The presence of CCTV offers reassurance to parents, fosters a secure learning environment, and promotes responsible behaviour amongst the children. It also aids in effective supervision, emergency preparedness, and facilitates the implementation of appropriate safety protocols. Overall, CCTV in primary schools is a valuable tool that enhances safety, security, and peace of mind for the entire school community. While the primary purpose of CCTV is for safety and security, we are committed to balancing its use with respect for privacy. CCTV will be used solely for security purposes and footage will be handled with the highest level of care and in compliance with relevant data protection regulations, including the General Data Protection Regulation (GDPR). Footage will be stored securely and accessed only by authorised personnel when necessary. This ensures that CCTV is used responsibly and transparently, with respect for the privacy of all individuals within the school community.

## **Purpose**

The purpose of this policy is to regulate the management, operation, and use of the CCTV system (Closed Circuit Television) at Crompton Primary School. The school uses CCTV images to prevent, identify, and reduce crime, as well as to monitor the school premises in order to provide a safe and secure environment for pupils, staff, and visitors, and to protect school property from loss or damage. CCTV surveillance at the school is intended for the following purposes:

- Protecting the school buildings and assets, both during and after school hours;
- Promoting the health and safety of staff, pupils, and visitors;
- Reducing incidents of crime and anti-social behaviour, including theft and vandalism;
- Supporting the Police in deterring and detecting crime;
- Assisting in identifying, apprehending, and prosecuting offenders.
- 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
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings

The system is owned and operated by the school, and its deployment is determined by the school's leadership team. The CCTV operates as a standalone system managed by the school.

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

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 the 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.

### **Relevant legislation and guidance**

This policy is based on:

#### **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 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

#### **Guidance**

Surveillance Camera Code of Practice (2021)

#### **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

#### **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.

Additionally, the proper authorisation forms from the Home Office will be completed and retained where necessary.

### **Location of the cameras**

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system.

The cameras are sited so that they only capture images (with the exception of the Head Teacher's Office, where audio and video recording is captured.) relevant to the purposes for which they have been installed, and care will be taken to ensure that reasonable privacy expectations are not violated. The school will make every effort to position the cameras so that their coverage is restricted to the school premises. CCTV will not be used in any regular internal pupil or staff areas, with the exception of corridors and the school hall.

Cameras are currently located in the following areas:

See attached plan

CCTV signage is displayed at site and building entrances, on school doors and property, and on the Headteacher's office door 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 not and will not be 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.

### **Roles and responsibilities**

#### **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.

#### **The headteacher**

The headteacher 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 having 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

### **The data protection officer (DPO)**

The 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 UK GDPR and Data Protection Act 2018

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 (ICO)

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 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

Receive and consider requests for third-party access to CCTV footage

### **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 daily

Ensure the data and time stamps are accurate weekly

### **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.

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

## **Storage of CCTV footage**

Footage will be retained for 21 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 21 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.

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

If footage or images are required to be saved as evidence, the following procedures apply: The required footage (digital or hard copy) will be stored securely in a restricted access location. Access to the data must be updated on the school's central log.

Only the footage required will be saved, any excess material must be deleted.

Any external requests to view CCTV data must be in writing to the Headteacher and where appropriate must be accompanied by the appropriate request form from the relevant agency.

The central log must be updated where data is released to an external authorised party and the person collecting must sign a release form.

## **Access to CCTV footage**

The school keeps a record of instances where CCTV footage is accessed. Access will only be given to authorised persons, for the purpose of pursuing the aims, or if there is a lawful reason to access the footage.

Access to recorded images will be restricted to staff authorised to view them and will not be made widely available. The Headteacher is responsible for supervising access to and maintenance of the CCTV system. The Headteacher may delegate the administration of the CCTV system to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need to-know basis. There will be no disclosure of recorded data to third parties, except for authorised personnel such as the Police and service providers to the school, where they reasonably need access to the data (e.g., investigators). If a Court order is granted for the disclosure of CCTV images, the school will comply with the order. However, careful consideration must be given to exactly what the Court order requires. If there are any concerns regarding disclosure, the Data Protection Officer should be contacted first, and appropriate legal advice may be sought. Requests for images must be made in writing to the Data Protection Officer.

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.

The school records the following information:

- Date of access
- Person accessing the footage
- Period of footage accessed
- Which zone/s within school have been viewed
- Reason for viewing
- Whether the footage is to be saved and for what reason
- Any authorised external parties requiring the data (e.g. police)
- Date of collection by authorised external parties

### **Staff access**

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

The headteacher: Mrs Gemma Croston

The DPO: Mr Justin Hardy

The system manager: Mrs Lois Hague / Mr David Smith

Anyone with express permission of the headteacher

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.

### **Subject access requests (SAR)**

According to the UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves. All requests should be made in writing to the Data Protection Officer via the Headteacher. Upon receiving SAR the school will immediately issue a receipt and will then respond within 1 calendar month.

Individuals submitting requests for access will be asked to provide sufficient information to help identify the relevant footage, such as time, date, and location.

The school does not have the facility to provide copies of CCTV footage; however, the applicant may view the footage if available.

The school reserves the right to refuse access to CCTV footage if doing so would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. 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 the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with a 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 [ICQ website](#).

### **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 headteacher 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 the UK GDPR.

All disclosures will be recorded by the DPO.

### **Responsibilities**

The Headteacher and Governors will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set by the school.
- Oversee and coordinate the use of CCTV monitoring for safety and security purposes within the school.
- Ensure that all existing CCTV monitoring systems are evaluated for compliance with this policy.
- Ensure that CCTV monitoring at the school is conducted in line with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV footage, in compliance with this policy.
- Maintain a record of access (e.g., an access log) for the release of any recorded material.
- Ensure that monitoring records are not duplicated for release.
- Ensure that the perimeter of view from fixed-location cameras conforms to this policy, both internally and externally.
- Ensure that all areas being monitored respect the privacy of individuals within the school, and that any infringement on privacy is avoided.
- Ensure that external cameras are non-intrusive in terms of their position and views of neighbouring residential housing, adhering to the principle of "Reasonable Expectation of Privacy."
- Ensure that monitoring footage is stored securely, with access restricted to authorised personnel only.
- Ensure that camera control does not infringe on an individual's reasonable expectation of privacy in public spaces.

### **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 Gemma Croston / Lois Hague.

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 done annually and whenever cameras are moved, or new cameras are installed.

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

### **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 cybersecurity 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

### **Complaints**

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

### **Monitoring**

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

### **Links to other policies**

Data protection policy

Biometric data policy

Privacy notices for parents/carers, pupils, staff, governors and suppliers

Safeguarding policy



### CCTV Cameras

- 8MP Fixed Turret 2.8mm (STROBE LIGHT & AUDIBLE WARNING)
- 8MP Fixed Turret 4mm (STROBE LIGHT & AUDIBLE WARNING)
- 4MP Varifocal Dome 2.8mm - 12mm.
- 8MP Fixed Dome 2.8mm
- OPTIONAL ADDITIONAL CAMERAS

