



Thameside Primary School: CCTV Policy

Approved by Governors: March 2026 (Review every 2 years)

Review date: May 2028

Thameside Primary School is a Rights Respecting School. School policies will respect the UN Convention on the rights of the child. The Health and Safety policy links to

Article 36: Children should be protected from any activity that could harm their development.

1. PURPOSE

The purpose of this policy is to regulate the management, operation and use of the Closed-Circuit Television (CCTV) system at **Thameside Primary School** (hereafter referred to as *the School*). The policy ensures that CCTV is used in a transparent, lawful and proportionate manner that supports the safety, security and effective management of the School.

The School recognises that CCTV systems have the potential to be privacy intrusive. Accordingly, a Data Protection Impact Assessment (DPIA) has been undertaken to evaluate whether the CCTV system represents a necessary and proportionate measure in achieving the School's legitimate aims. The findings of the DPIA have informed both the use of CCTV and the development of this policy.

In implementing and operating CCTV, the School is committed to:

- Maintaining transparency in all aspects of CCTV operation
- Upholding integrity in the handling and storage of recorded data
- Ensuring full compliance with data protection legislation
- Maintaining proper governance and accountability
- Ensuring ethical and lawful practice
- Operating with openness regarding the purpose and scope of CCTV
- Ensuring all actions are legitimate, documented and appropriately authorised

This policy will be reviewed annually, or sooner where necessary. Reviews will also take place whenever new CCTV equipment is introduced, accompanied by an updated risk assessment. In all cases, the policy will be reviewed at least once every two years.

2. OBJECTIVES

The objectives of the School's CCTV system are to:

- (a) Detect and protect vulnerable areas of the School and its property from anti-social behaviour, vandalism or other harmful acts.
- (b) Increase personal safety and promote a secure environment for pupils, staff and visitors.
- (c) Protect School buildings, grounds and assets from crime.
- (d) Support the School and the police in the prevention and detection of crime.
- (e) Establish the cause of accidents or adverse incidents and support actions to prevent recurrence.
- (f) Assist in the effective management and safeguarding of the School.

3. LOCATIONS OF CCTV CAMERAS

A CCTV warning sign will be clearly and prominently placed near to the cameras and children and school staff will be briefed about the use of the cameras and their intended purpose.

Non recording cameras

A CCTV camera is installed by the main entrance to the School in order that staff working in the office area may view persons seeking access to the School before pressing the door release button on their phones.

This enables them to make a judgement as to whether to prevent entry to a person or persons who may pose a danger to themselves, other staff or pupils. Images will be displayed on the computer screens of staff working in the school office in real-time. There will be no recording of images. This is accessed through a web-based programme.

Recording cameras

The school have 3-hard wired recording CCTV cameras recording

Make/Model: 4 MP AcuSense Fixed Turret Network Camera(P)

Camera Location	What is area of view?	What it will not capture?
Camera facing from quad to playground near the Year 4 outside Donald Toilets	Captures children or persons entering the playground and entering/exiting the pupils outside toilets	It does not capture the images inside the Donald Block external toilets. You will not see inside the toilets or inside the cubicles.
Camera facing over field towards Elliott's Way	Field/ new Playground area	Will not overlook road or neighbouring houses
Camera fitted on corner of new build, external to year 5 Dolphin classroom facing diagonally across the playground (near Ball zone)	Will capture video recording of children playing on playground or any other persons walking by this camera.	Will not overlook houses

CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

CCTV Cameras are installed in high out of reach positions. Signs are predominantly displayed where relevant, so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV.

4. STATEMENT OF COMPLIANCE

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Information Commissioner's Code of Practice. The school are registered with the ICO.

Key Aspects of Current ICO Guidance & Best Practices:

- **Proportionality & Purpose:** CCTV must be used only to address a clear, specific need (e.g., vandalism, violence). It should not be used in areas with a high expectation of privacy, such as toilets or changing rooms.
- **DPIA Requirement:** Schools must conduct a [Data Protection Impact Assessment \(DPIA\)](#) before installing or changing surveillance systems to demonstrate compliance with UK GDPR.
- **Signage & Privacy Notices:** Cameras must be clearly visible and accompanied by prominent signs explaining that CCTV is in use, the purpose, and who to contact.
- **Data Retention & Access:** Footage should only be kept for the minimum time necessary, no longer than 30 days. Access to recorded footage must be restricted to authorised personnel.
- **Audio Recording:** Generally discouraged, as it is difficult to justify recording conversations under GDPR.

The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property,

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment or solely for TV or press reporting purposes.

The planning and installation design has endeavored to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

CCTV images are not retained for longer than necessary, considering the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.

Recorded images will only be retained longer than 30 days if express written authority is granted by the police as part of an ongoing police investigation or legal case.

5. SYSTEM MANAGEMENT

Access to images will be restricted to staff authorised to view them.

Access to the CCTV system and data shall be password protected and will be kept in a secure area, SEN upstairs office.

The Headteacher will act as System Manager and take full responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by the School Business Manager.

The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

It is intended that only the School Business Manager and/or the Headteacher will access the CCTV recorded devices to play back recordings. Footage will be viewed with minimum two authorised people present.

Footage seen will be accurately documented to ensure information is captured and relayed correctly to any persons responsible for investigating. Details of the person(s) viewing the footage will be declared for purpose of audit and retention of video records.

The CCTV system is designed to be in operation 24/7 every day of the year though the school does not guarantee that it will be working during these hours.

The System Manager or School Business Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by providing clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those with authority, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

Details of all access to viewing footage and authorised visitors, for example the police, will be recorded in a system log book including time/date of access and details of images viewed and the purpose for so doing.

Downloading Captured Data Onto 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 used to record events from the hard drive must be prepared in accordance with the following procedures:

- (a) Each downloaded media must be identified by a unique mark.
- (b) Before use, each downloaded media must be cleaned of any previous recording.
- (c) The System Manager will register the date and time of downloaded media insertion, including its reference.
- (d) Downloaded media 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.
- (e) If downloaded media is archived the reference must be noted.
- (f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised senior leaders. 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 shall be preferable if possible, 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 they are needed by the police.

Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's data protection officer.

Complaints About The Use Of CCTV

Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

Request For Access By The Data Subject

The Data Protection Act provides Data Subjects — those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Headteacher of the school.

Public Information

Copies of this policy will be available from the school office or the school's website.

5. CCTV RETENTION

Non recording camera

The CCTV camera is used for live viewing only and no footage is retained.

Recording cameras

CCTV images are not retained for longer than necessary, considering the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.

6. RESPONSIBILITIES

The Headteacher will ensure use of the CCTV system is implemented in accordance with this policy.

7. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The installation of the system will be subject of a DPIA that will be reviewed by the School's Data Protection Officer (DPO) Judicium.

Reviewed by: Vick Lucas, School Business Manager