OAKLANDS SCHOOL CCTV POLICY

Document Number 1



CCTV Policy

1. Introduction

Oaklands School recognises that CCTV systems can be privacy intrusive.

Review of this policy shall be repeated regularly and whenever new equipment is introduced a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

2. Objectives

The purpose of the CCTV system is to assist the School in reaching these objectives:

(a) To protect pupils, staff and visitors against harm to their person and/or property.
(b) To increase a sense of personal safety and reduce the fear of crime.
(c) To protect the school buildings and assets.
(d) To support the police in preventing and detecting crime.
(e) To assist in identifying, apprehending and prosecuting offenders.
(f) To assist in establishing a cause of accidents and other adverse incidents and prevent reoccurrence.
(g) To assist in managing the School.

3. Purpose of This Policy

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at the School. The 'HIKVISION CCTV' system is used by the School and is comprised of the following:

Camera type	Location	Sound Yes/No	Swivel or fixed
Example: HikVision	Main Buildings	Yes OFF	Fixed

The cameras are positioned in the following locations:

Location	Number of cameras
Example: **Main Buildings,**	8
Chimney Stack, roof, facing car park. (EXTERNAL)	1
Room 10-GF-134 Staff & Admin (EXTERNAL)	2
Room 10-GF-101 Year 6 (EXTERNAL)	2
Room 10-GF-103 Year 4 (EXTERNAL)	1
Room 10-GF-133 Circulation Entrance (INTERNAL)	1
Room 10-GF-122 Main Hall (INTERNAL)	1

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

4. Statement Of Intent

CCTV Cameras are installed in such a way that they are not hidden from view. 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. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

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

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 of 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.

The planning and design have endeavoured 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.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after 30 days.

Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than twenty days.

(Continued)

5. System Management

Access to the CCTV system and data shall be password protected or, in the case of the Premises Office, in a locked room.

The CCTV system will be administered and managed by the Premises who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Premises Department, the system will be managed by the IT Department.

The system and the data collected will only be available to the Premises Department, the IT Department, and appropriate members of the senior leadership team as determined by the Headteacher.

The CCTV system is designed to be in operation for 24 hours each day, every day of the year, though the School does not guarantee that it will be working during these hours.

The Premises 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 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 mentioned above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of the purpose of any person making such request. Where any doubt exists access will be refused.

Details of all visits and visitors will be recorded in a system log book including time/date of access and details of images viewed and the purpose for so doing.



6. 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 Premises Department, the IT Department, 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 and 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.

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.

7. Complaints

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

8. 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 data held about themselves, including those obtained by CCTV. Requests for such data should be made to the School's GDPR Officer, using the following email address: admin@oaklands.herts.sch.uk

9. Public Information

Copies of this policy will be available to the public from the school office or the school website, Email – admin@oaklands.herts.sch.uk

Version Control	
Implementation Date	**29th May 2025**
Next Review Due	**1st June 2026**

Ownership and Consultation	
Document Sponsor	**Mr Tom Hassan (HeadTeacher)**
Document Author	**Mr Kevin Stammers (Site Manager)**
Specialist Advisor	**Admin**

Guidance Version Control		
Name Of Document	**Version**	**Last Review date**
Oaklands School CCTV Policy	N/A	May 2025