# CCTV Policy

| | |
|---|---|
| Policy Reference | CCTV |
| Committee | |
| Completed Review Date | November 2024 |
| Policy Owner | Data Protection Lead |
| Ratified by Governors | |
| Next Review Due | October 2026 |

MONITORING, EVALUATION AND REVIEW

This policy will be reviewed when there are changes in the law or at least every two years, to assess implementation and effectiveness in line with DfE guidance September 2022.

## Contents

## Preface

Chiltern Hills Academy is a learning environment at the heart of its community. We encourage every person in our community to:

**Create, Aspire and Excel to 'Live life in all its fullness' (John 10:10)**

We achieve this through our dedication to the seven Christian values of love, hope, self-discipline, compassion, forgiveness, respect and honesty.

We are a community in which staff, students and parents work collaboratively to develop a learning environment and organisation which is spiritual, safe, innovative, creative and exciting. All members of the Academy are motivated and inspired by the vision to give their best and to play a full part in the life of the school and in their own developing lives.

The Governors at Chiltern Hills Academy are committed to achieving the vision and values. They oversee and monitor this policy to ensure that this is being achieved.

## 1. Objectives

### 1.1 Review of Policy

We aim to conduct reviews no later than every two years. In addition, whenever new equipment is introduced, a review will be conducted, and a risk assessment put in place.

### 1.2 The purpose of the CCTV system is to assist the school in reaching the following 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, both during and after school hours
(d) To support the police in preventing and detecting crime;
(e) To assist in identifying, apprehending and prosecuting offenders;
(f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence; and
(g) To assist in managing the school and investigating situations where school rules are not respected.

## 2. Purpose of the policy

The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Chiltern Hills Academy. CCTV systems are installed in our premises for the purpose of enhancing security of the building and its associated equipment. It also creates an awareness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

### 2.1 Camera Location

The system comprises a number of cameras located on and within the school buildings, within corridors and at strategic points throughout the school premises, principally at the entrance and exit points and the play areas around the school. Some cameras are on a movement timer as they cover a vast area such as the Artificial Grass Pitch.

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

## 3. Statement of intent

3.1 CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Warning signs, as required by the Code of Practice of the Information Commissioner, will be clearly visible in main reception and make clear who is responsible for the equipment. 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.

3.2 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 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.

3.3 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 or cover the entire site.

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

3.5 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 a period of up to 90 days.

Any downloaded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed or incident reported) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

## 4. System management

4.1 The CCTV system will be kept in a restricted secure area with access to the system and data additionally password protected.

4.2 The CCTV system will be administered and managed by our Site Manager 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 Site Manager, the system will be managed by his deputy in the Site team.

4.3 The system and the data collected will only be available to the Systems Manager, their deputy and members of the senior leadership team as determined by the Principal. The Principal can authorise Key Stage Leads and Year Leads to review specific incidents.

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

4.5 The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that the cameras are functional.
Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

4.6 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.

4.7 Where a person other than those mentioned above requests access to the CCTV data or system, the System Manager must confirm with the Principal. Where any doubt exists, access will be refused.

4.8 Details of all authorised access requests will be recorded in a system logbook including time/date of access and details of images viewed and the purpose for so doing.

## 5. Downloading captured data on to other media

5.1 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.

5.2 Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her deputy and the Principal 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.

5.2.1 A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

5.2.2 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 needed by the police.

5.3 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.

## 6. Complaints about the use of CCTV

In accordance with our **Complaints and Resolutions Policy** any complaints in relation to the school's CCTV system should be addressed to the Principal.

## 7. Requests for subject access requests (sars)

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 Data Protection Officer. The requested data if available will be disclosed in the format of still images with all third parties redacted.

## 8. Public information

Copies of this policy will be available to the public from the school office and the school website.