# CIRENCESTER KINGSHILL SCHOOL

## CCTV SYSTEM POLICY

**The law states that a CCTV system can be used to monitor the School's premises, providing our system complies with the Data Protection Act.**

### 1. INTRODUCTION

Cirencester Kingshill School takes its responsibility towards the safety of staff and pupils very seriously - to that end:

1.1 The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Kingshill School, hereafter referred to as 'the School'.

1.2 The system comprises a number of fixed and dome cameras located around the School site. All cameras are monitored within the School.

1.3 This Policy has been drafted in compliance with the requirements of the General Data Protection Regulation.

1.4 The Policy will be subject to review annually, to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the School.

### 2. OBJECTIVES OF THE CCTV SCHEME

2.1 (a) To protect the School buildings, their assets and maintain a safe environment.
(b) To increase personal safety and reduce the fear and incidence of crime.
(c) To support the Police in a bid to deter and detect crime.
(d) To assist in identifying, apprehending and prosecuting offenders.
(e) To protect members of the public and private property.
(f) To assist in managing the School and ensuring the welfare of staff and pupils.

### 3. STATEMENT OF INTENT

3.1 The ICT Systems Manager will ensure that the CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements of the Data Protection Act, the Commissioner's Code of Practice for CCTV (2008) and the Surveillance Camera Code of Practice 2013 (published by the Home Office).

3.2 The School will treat the system and all information, documents and recordings obtained and used as data which are protected by the General Data Protection Regulation and will be processed in accordance with the requirements of the regulation.

3.3 Cameras will be used to monitor activities within the School and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the School, together with its visitors.

3.4 Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

3.5 Unless an immediate response to events is required, staff investigating a criminal offence must not direct cameras at an individual, their property or a specific group of individuals, without police involvement.

3.6 Recordings or knowledge secured as a result of CCTV will not be used for any commercial purpose. Footage will only be released to the media for use in the investigation of a specific crime and with the agreement of the Headteacher and written approval of the police. Footage will never be released to the media for purposes of entertainment.

3.7 The planning and design has endeavoured to ensure that the Scheme 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.

3.8 Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the School CCTV where the system is active.

## 4. THE DATA PROTECTION PRINCIPLES

4.1 Data collected from CCTV will be processed in accordance with the principles of the General Data Protection Regulation. As such, all data will be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed

(d) Accurate and where necessary, kept up to date

(e) Kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are processed

(f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

## 5. OPERATION OF THE SYSTEM

5.1 The Scheme will be administered and managed by the ICT Systems Manager, in accordance with the principles and objectives expressed in the code.

5.2 The day-to-day management will be the responsibility of the ICT Systems Manager.

5.3 The CCTV system will be operated 24 hours each day, every day of the year. Images are captured with detection of motion.

## 6. CONTROL ROOM

6.1 The ICT Systems Manager will be responsible for the CCTV System and will ensure it meets the needs of the School.

6.2 The ICT Systems Manager is responsible for the tendering of the CCTV maintenance contract.

6.3 The ICT Systems Manager will check and confirm the efficiency of the system at least on a twice-weekly basis and in particular that the equipment is properly recording and that cameras

are functional. Any problems with the cameras should be reported to the ICT Systems Manager.

6.4 Access to the CCTV facilities will be strictly limited to the Site Manager: Premises Development and Security, ICT Systems Manager, Senior Leadership Team (SLT) and the Heads of Year (HOY). The system is password protected and kept in a secure and locked office.

6.5 Control operators (Site Manager: Premises Development and Security, ICT Systems Manager, SLT) must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused.

6.6 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption.

6.7 If out of hours emergency maintenance arises, the Site Manager: Premises Development and Security must be satisfied of the identity and purpose of contractors before allowing entry.

6.8 When not manned, the facility will be kept secured using an access control system. Entry to the facility will be monitored via this system.

6.9 Other administrative functions will include maintaining logs and hard disc space, filing and maintaining occurrence and system maintenance logs. The ICT Systems Manager is responsible for these functions.

6.10 Emergency procedures will be used in appropriate cases to call the Emergency Services.

## 7. MONITORING PROCEDURES

7.1 Camera surveillance may be maintained at all times.

7.2 A monitor is installed in the Control facility to which pictures will be continuously recorded which is kept secure and locked when not in use.

7.3 If through routine maintenance, or if CCTV footage is accessed for some other reason, it is discovered that a member of staff has been undertaking a criminal activity or breaching school security this could result, after an investigation, in the Conduct Procedure being activated or, in the case of a criminal activity, the police being informed.

7.4 Any covert surveillance would only be undertaken after police authority has been obtained by the Headteacher or the Deputy Headteacher where there are grounds for suspecting criminal activity or equivalent.

## 8. RECORDED MATERIAL PROCEDURES, RECORD KEEPING AND INCIDENT LOGS

8.1 Any recordings required for criminal evidential purposes will be produced and stored by the ICT Systems Manager (or the Site Manager: Premises Development and Security in his absence) on the advice of the police.

8.2 Recorded materials may be viewed by / released to third parties, only in the following circumstances, and then only to the extent required by law.

- The police, where any images recorded would assist in a specific criminal inquiry.
- Prosecution agencies, such as the Crown Prosecution Service (CPS).
- Relevant legal representatives such as lawyers and barristers.

- Persons whose images have been recorded and retained, and where disclosure is required by virtue of data protection legislation, or the Freedom of Information Act.

8.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register maintained by the ICT Systems Manager will be made available for this purpose.

8.4 Viewing of recorded materials by the Police must be recorded in writing and in a log book.

8.5 Should recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 7.9 Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the School, and both the recorded material and information contained on it are to be treated in accordance with this document.

8.6 The School retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material this will be produced from the secure recorded material store, complete in its sealed bag.

8.7 If the Police require the School to retain the stored recorded materials for use as evidence in the future, such recorded materials will be properly indexed and properly and securely stored until they are needed by the Police.

8.8 Requests for access or disclosure will be recorded and the Headteacher will make the final decision as to whether the recorded images may be released to persons other than the police.

8.9 The School will maintain adequate and comprehensive records relating to the Management of the system and incidents.

## 9. RETENTION OF DATA

9.1 There are no specific guidelines about the length of time data images should be retained. Consequently, the period of retention will be determined locally, will be documented and understood by those operating the system and will be for the minimum period necessary to meet the objectives of the CCTV scheme. A period of 30 days is considered adequate unless determined otherwise.

9.2 Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.

9.3 Measures to permanently delete data should be clearly understood by persons that operate the system.

9.4 Systematic checks should be carried out to ensure the deletion regime is strictly followed.

## 10. BREACHES OF THE POLICY (including breaches of security)

10.1 Any breach of this Policy by school staff will be initially investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action.

10.2 Where any breach of this Policy involves allegations against the Headteacher, the Chair of Governors will be informed and he / she arrange for the appropriate initial investigations to be carried out in order for him / her to take the appropriate disciplinary action.

10.3 Any serious breach of the Policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

## 11. COMPLAINTS

11.1 Any complaints about the School's CCTV system should be addressed to the Headteacher.

## 12. PUBLIC INFORMATION

12.1 Copies of this Policy will be available to the public from the School Office.

## 13. ACCESS BY THE DATA SUBJECT

13.1 The General Data Protection Regulation provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

13.2 Individuals have the right to submit a subject access request in order to gain access to their personal data.

13.3 If the individual is not the focus of the footage i.e. they have not been singled out or had their movements tracked then the images are not classed as 'personal data' and the individual is not entitled to the image under the provisions of Subject Access Requests.

13.4 In such instances, the School will verify the identity of the individual making the request before any information is supplied.

13.5 All requests will be responded to without delay, and at the most within one month.

13.6 Requests for access or disclosure will be recorded and the Headteacher will make a final decision as to whether recorded images may be released to persons other than the police.

Summary of Key Points

- This Policy will be reviewed annually.
- The CCTV system is owned and operated by the School.
- The Control system is not open to visitors except by prior arrangement and with good reason.
- Liaison meetings may be held with the Police and other bodies.
- Any recording will be used properly, indexed, stored on hard drive and removed after a period of one month.
- Footage may only be viewed in the presence of / with the authority of the Control Operators and / or the Police.
- Footage required as evidence will be managed in accordance with advice in this Policy.
- Footage will not be made available to the media for commercial or entertainment purposes.
- Footage will be erased from the hard drives and over recorded.
- Any breaches of this Policy will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Where a breach involves allegations against the Headteacher, the Chair of Governors will arrange for appropriate investigations to be undertaken and in event of a serious breach will arrange for an independent investigation to be carried out.
- Breaches of this Policy and remedies will be reported to the Headteacher.

**CIRENCESTER KINGSHILL SCHOOL**

**CCTV SYSTEM POLICY**

Reviewed by S Gardiner (Business Manager) / D Evans (ICT Systems Manager) September 2020 (Date)

Adopted by Governors _____ (Sign) _____ (Date)

Review date November 2021