# Cranborne Middle School

# CCTV Policy

## 1. Introduction

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

1.2 The system comprises a number of fixed, dome and remote cameras located around the school site. All cameras are monitored via access to secure servers and are only available to selected senior staff (authorised users) on the Administrative Network.

1.3 This policy follows Data Protection guidelines and the Information Commissioners Office CCTV code of practice (May 2015).

1.4 The Code of Practice will be subject to review bi-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 and their assets

(b) To increase personal safety and reduce the fear 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

(g) The system does not have sound recording capabilities

## 3. Statement of intent

3.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act and will seek to comply with the requirements of the Data Protection Act, GDPR and the Commissioner's Code of Practice.

3.2 The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

3.3 Cameras will be used to monitor activities within the school and its car park 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.

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

3.4.2 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without authorisation being obtained, as set out in the Regulation of Investigatory Power Act 2000.

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

3.6 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.

3.7 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.

## 4. Operation of the system

4.1 The Scheme will be administered and managed by the Headteacher, in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the Senior Leadership Team, ICT Support, Office staff and the caretaker during the day, with the caretaker also managing out of hours and at weekends.

4.3 The main CCTV system will be operated 24 hours each day, every day of the year.

4.4 Recordings are stored on hard drives for 30 days (with the exception of remote cameras) and are wiped at expiry or retained for investigatory purposes if required.

## 5. System functionality & Access

5.1 The IT Technician will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV system will be strictly limited to the SLT, ICT Support, Office staff and the Site Team (Operators) within their designated area of work only.

5.3 Unless an immediate response to events is required, authorised staff must not direct cameras at an individual or a specific group of individuals.

5.4 Visitors and other contractors wishing to enter areas of work where images are being displayed will be subject to particular arrangements as outlined below.

5.5 Operators must satisfy themselves over the identity of any other visitors who view images and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be logged and signed off before recordings are viewed.

5.6 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the System Manager, or Senior Leader and must be accompanied by them throughout the visit.

5.7 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

5.8 If out of hours emergency maintenance arises, the Operators must be satisfied of the identity and purpose of contractors before allowing entry.

5.9 Access to the servers (physically) is limited to the Operators via unique accounts which are password protected. Server rooms are secured both during the working day and when not manned.

5.10 Other administrative functions will include maintaining recordings and hard disc space, filing and maintaining occurrence and system maintenance logs.

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

## 6. Liaison

6.1 Liaison meetings may be held with all bodies involved in the support of the system.

## 7. Monitoring procedures

7.1 Camera surveillance may be maintained at all times.

7.2 Device hard drives are used to record pictures continuously.

## 8. USB procedures

8.1 In order to maintain and preserve the integrity of the USB's used to record events from the hard drive and the facility to use them in any future proceedings, the following procedure for their use and retention must be strictly adhered to:

Media required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store. If 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, signed by the controller, dated and returned to the evidence store.

8.2 Recordings may be viewed by the Police for the prevention and detection of crime or for supervisory purposes, authorised demonstration and training.

8.3 A record will be maintained of the release of media to the Police or other authorised applicants. A register will be available for this purpose.

8.4 Viewing of recordings by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under the Data Protection Act.

8.5 Should a recording be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 of this Code. Media will only be released to the Police on the clear understanding that the media remains the property of the school, and both the media and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Police to pass to any other person the media or any part of the information contained thereon. On occasions when a Court requires the release of an original recording this will be produced from the secure evidence store, complete in its sealed bag.

8.6 The Police may require the school to retain the stored media for possible use as evidence in the future. Such media will be properly indexed and properly and securely stored until they are needed by the Police.

8.7 Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Headteacher. In these circumstances the media will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

## 9. Breaches of the code (including breaches of security)

9.1 Any breach of the Code of Practice by school staff will be initially investigated by the Headteacher, in order for them to take the appropriate disciplinary action.

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

## 10. Assessment of the scheme and code of practice

10.1 Performance monitoring, including random operating checks, may be carried out by the System Manager and the Site Manager.

## 11. Complaints

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

11.2 Complaints will be investigated in accordance with Section 9 of this Code.

## 12 Access by the Data Subject

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

12.2 Requests for Data Subject Access should be made to the Headteacher.

12.3 All requests should be made in writing to the Headteachers PA who can be contacted by email to dwarner@cranbornemid.dorset.sch.uk. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: time, date and location.

12.4 The School does not have a facility to provide copies of CCTV footage but instead the applicant may view the CCTV footage if available.

12.5 The School will respond to requests within 30 days of receiving the request but if a request is received outside of the School term this may not be possible.

12.6 The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

## 13. Incident Review Procedure

13.1 Requests to review incidents can only be made by school staff.

13.2 Reviews will be carried out by either the Headteacher, SLT or year leader with support from the IT Technician.

13.3 Reviews will take place within the IT Office.

## 14. Public information

Copies of this Code of Practice will be available to the public from the School Office and the Headteacher.

Summary of Key Points

• This Code of Practice will be reviewed every two years.

• The CCTV system is owned and operated by the school.

• The viewing of images is not open to visitors except by prior arrangement and good reason.

• Liaison meetings may be held with the Police and other bodies.

• Recording media will be used properly, indexed, stored and destroyed after appropriate use.

• Recordings may only be viewed by Authorised School Officers and the Police.

• Media required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.

• Recordings will not be made available to the media for commercial use or entertainment.

• Media no longer required will be disposed of securely by incineration.

• Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the corporate policies and procedures and must be logged.

• Any breaches of this code will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.

• Breaches of the code and remedies will be reported to the Headteacher.

This document was produced September 2020

Monitoring

The Health and Safety governor is responsible for auditing the CCTV System policy and procedures.

The policy will be reviewed every two years.

Ratified by the FGB December 2020