Cranborne Middle School
CCTV Policy

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Cranborne Middle School (CMS), hereafter referred to as 'the School'. The system comprises a number of fixed cameras located around the school site. All cameras are monitored via access to secure servers and are only available to selected staff if required for a particular purpose. This policy follows Data Protection guidelines and the Information Commissioners Office CCTV Code of Practice (May 2015). The Policy will be subject to review bi-annually to include consultation as appropriate with interested parties. The CCTV system is owned by the school.

2. Objectives of the CCTV System

- To protect the school buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the school

3. Statement of Intent

The CCTV Scheme has been registered with the Information Commissioner under the terms of the Data Protection Act and the School will comply with the requirements of the Data Protection Act, GDPR and the Commissioner's Code of Practice. The School will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act. 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, staff, pupils and visitors.

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

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.

The planning and design has 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 have been placed at all access routes to areas covered by the school CCTV.

4. Operation of the System

The Scheme will be administered and managed by the Headteacher, (The Controller) in accordance with the principles and objectives expressed in this policy. The day-to-day monitoring of the system will be the responsibility of the IT Technician though the School Office has the ability to monitor certain cameras. The system will be operated 24 hours each day, every day of the year. Recordings are stored on hard drives for 30 days and are wiped at that point or retained for investigatory purposes if required as directed by the Controller.

5. System functionality and Access

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. He/she is responsible for the proper operation of the system and will report any concerns he has to the Controller.

Anyone requiring access to the System is to seek authority from the Controller in the first instance. Such access having been authorised will be executed through the IT Technician who is to confirm with the Controller personally that access has been agreed, before allowing any access.

In allowing access, the Controller is first to consider the justification of the request, the needs of the School and if any safeguarding issues apply. If necessary, he/she is to seek legal advice before allowing access.

The IT Technician is responsible for maintaining a formal written record (The CCTV Log) of who obtains access to the System, when and for what purpose. This record is to be presented to the Controller quarterly for signature. Access to the system must be password protected and in a secure server room which does not allow others to view the system when it is viewed.

The IT Technician is to record any access to the system required by maintenance contractors supporting the system in the CCTV Log. He is to confirm their identity and monitor their work throughout to ensure that they do not access CCTV data except as specifically required to support the system. Server rooms are to be secured both during the working day and when not manned.

6. Transfer of Data - Procedures

- The IT Technician is responsible for the security and integrity of all CCTV data transferred from the system. In order to maintain and preserve the security and thus the integrity of data transferred from the hard drive of the system, the following procedure must be strictly adhered to:
- Transfers of CCTV data can only be authorised by the Controller, such access is to be carried out by the IT Technician who is to record the event in the CCTV Log. Media required by the Police for evidential purposes must be sealed, witnessed, and signed by the Controller, dated and stored in a separate, secure storage. 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 secure store.
- Recordings may be viewed by the Police for the prevention and detection of crime or for supervisory purposes, authorised demonstration and training. Such viewing would normally be authorised by the Controller and again a record kept.
- A record will be maintained of any release of media to the Police or other authorised applicants in the CCTV Log. 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 the Information Commissioners Code of Practice. The school also retains the right to refuse permission for the Police to pass CCTV data 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 store, complete in its sealed bag.
- The Police may require the school to retain stored media for possible use as evidence in the future. Such media will be properly indexed and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Controller. 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.

7. Assessment of the System and this Policy

Performance monitoring, including random operating checks, may be carried out by the Controller and the IT Technician. Such checks are to be logged.

8. Complaints and Breaches of this Policy (*including breaches of security*)

Any complaints or breaches of this policy should be addressed to the Controller (Headteacher) who will investigate the complaint in the first instance and take the appropriate action.

9. Access by the Data Subject

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. Such requests for Data Subject Access should be made to the Controller (Headteacher). 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 e.g: time, date and location.

The applicant may view the CCTV footage if available. The School will respond to requests within 30 days of receiving the request but if a request is received outside of a School term this may not be possible. 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 or safeguarding issues are involved and to seek legal advice before making this facility available.

10. Incident Review Procedure

Requests to review incidents made by school staff are to be addressed to the Controller in the first instance. Reviews will be carried out by the Controller, with support from the IT Technician. The controller will then decide if it is appropriate for an incident to be reviewed by another member of staff. Reviews will take place within the IT server room.

11. Public information

Copies of this Policy will be available to the public from the School on written request.

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

The policy will be reviewed every two years.

Dated: December 2021