Produced by:	**JHY:**
Responsible Gov Committee:	**H&S**
Last Amended	**November 2018**
Date approved by FGB	**28.11.2018**
Date for Review:	**October 2020**

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 Crofton School hereafter referred to as 'the school'.
The system comprises a number of fixed and dome cameras located around the school site. All cameras are monitored from a central control room and licensed software and are only available to selected senior staff on the Administrative Network.

This policy follows GDPR guidelines and will be subject to review annually to include consultation as appropriate with interested parties.

The CCTV system is owned by the school.

2. Objectives of the CCTV scheme

- 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

This CCTV policy will seek to comply with the requirements both of the General Data Protection Regulation (GDPR) and the Commissioner's Code of Practice. The school will treat the CCTV system and all information, documents and recordings obtained and used as data which are protected by the relevant legislation.

Cameras will be used to monitor activities within the school, 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.

Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property. 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 an authorisation being obtained using the school's forms for Directed Surveillance to take place, 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. Footage will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Footage will never be released to the media for purposes of entertainment.

The planning and design of the CCTV system 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.

Warning signs, as required by the Code of Practice of the Information Commissioner (ICO) 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 Operations Director, in accordance with the principles and objectives expressed in the (ICO) code. The day-to-day management will be the responsibility of both the Senior Leadership Team (SLT), Network & IT Team and the Senior Site Manager during the day and the Site Team out of hours and at weekends.

The Control Room will only be staffed by Network Team and the Premises Team.

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

5. Control Room

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

Access to the CCTV Control Room will be strictly limited to the SLT and the Senior Site Manager. Unless an immediate response to events is required, staff in the CCTV Control Room must not direct cameras at an individual or a specific group of individuals.

Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below. Control Room Operators 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. Details of all visits and visitors will be endorsed in the Control Room log book.

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 his deputy and must be accompanied by him throughout the visit. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

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

There must always be at least one Control Room Operator present within the Control Room out of hours and weekends or the Control Room must be locked. During the working day when not manned the room must be kept secured.

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

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

6. Monitoring procedures

Camera surveillance may be maintained at all times. A monitor is installed in the Control Room to which pictures will be continuously recorded.

If covert surveillance is planned, it can only be undertaken by the police or the Council using the appropriate authorisation forms.

7. Recording procedures

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

a. Each USB must be identified by a unique mark.
b. Before using, each USB must be cleaned of any previous recording.
c. The controller must register the date and time of USB insert, including reference.
d. If the USB is archived the reference must be noted.

Recordings may be viewed by the police for the prevention and detection of crime and authorised officers of the Council. A record will be maintained of the release of recordings to the police or other authorised applicants. A register will be available for this purpose.

Should a recording be required as evidence, a copy may be released to the police under the procedures described in the above bullet points of section 8 of this policy. Recordings will only be released to the police on the clear understanding that the recording remains the property of the school, and both the recording and information contained on it are to be treated in accordance with this policy. The school also retains the right to refuse permission for the police to pass to any other person the recording 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.

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

Applications received from outside bodies (for example solicitors) to view or release recordings will be referred to the Headteacher. In these circumstances USB's 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.

8. Breaches of the code (including breaches of security)

Any breach of this policy or the ICO Code of Practice by school staff will be initially investigated by the Operations Director, in order for them to take the appropriate disciplinary action.

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

9. Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by the Network Manager.

10. Complaints

Any complaints about the school's CCTV system should be addressed to the Headteacher. Complaints will be investigated in accordance with Section 9 of this policy

11. 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. Requests for data subject access should be made in accordance with the GDPR and on an application form available from the Headteacher.

12. Public information

Copies of this policy will be available to the public from the School Office and the Operations Director

Summary of Key Points

a. This Code of Practice will be reviewed annually.
b. The CCTV system is owned and operated by the school.
c. The Control room will not be manned out of school hours.
d. The Control Room is not open to visitors except by prior arrangement and good reason.
e. Recordings will be properly indexed, stored and destroyed after appropriate use.
f. Recordings may only be viewed by authorised Council and school officers, Control Room staff and the police.
g. Recordings required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
h. Recordings will not be made available to the media for commercial or entertainment.
i. USB's will be disposed of securely by incineration.
j. Any breaches of this policy will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
k. Breaches of the policy and remedies will be reported to the Headteacher.