

# Great Baddow High School



## CCTV POLICY

<b>RATIFIED by :</b>	<b>GOVERNING BODY</b>
<b>REVIEWED by :</b>	<b>PAUL DRAPER</b>
<b>REVIEW DATE :</b>	<b>SPRING TERM 2018</b>
<b>NEXT REVIEW :</b>	<b>SPRING TERM 2020</b>



# CCTV POLICY

## INTRODUCTION

- 1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Great Baddow High School, hereafter referred to as 'the school'.
- 1.2. The system comprises of **31** (Capacity for 32) cameras located in and around the school site. The system is not monitored. One screen in the main office displays rolling images of all cameras (excl. internal toilets in Main). The following staff have access to the system which enables them to monitor or review images should an incident occur or investigation be needed. An electronic access log is kept which could be used to indicate any excessive use or unusual activity of the system.

- SLT
- Network Managers
- Nominated Office/Student Admin. Staff
- Heads and Assistant Heads of Year

CCTV footage containing images of other students will not be shown to either students or parents.

- 1.3. This Policy follows Data Protection Act guidelines.
- 1.4. The School Policy will be subject to review bi-annually to include consultation as appropriate with interested parties.

## 2. OBJECTIVES OF THE CCTV SYSTEM

- 2.1. To improve security and access to the school site.
- 2.2. To protect pupils, staff and visitors.
- 2.3. To increase personal safety and deter crime including vandalism.
- 2.4. To protect the school buildings and assets.
- 2.5. Without prejudice, to protect the personal property of pupils, staff and visitors.
- 2.6. To support the police in preventing and detecting crime (at the discretion of the Head teacher)
- 2.7. To assist in identifying offenders.
- 2.8. To assist in managing student behaviour
- 2.9. To review reported incidents

### **3. STATEMENT OF INTENT**

- 3.1. The CCTV system will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.
- 3.2. The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- 3.3. Cameras will be used as specified in 2. above within the school and its grounds.
  - 3.3.1. The system has been designed to prevent observation on adjacent private homes, gardens and other areas of private property.
- 3.4. The monitoring or viewing of images from areas where an individual would have an expectation of privacy (currently N/A) should be authorised by the Head teacher or the Assistant Head responsible for Safeguarding.
- 3.5. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
  - 3.5.1. Images will never be released to the media for purposes of entertainment.
  - 3.5.2. Images will only be released to the media for use in the investigation of a specific crime at the request of and with the written authority of the police, subject to the Head teacher's discretion.
- 3.6. 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.
- 3.7. Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site.

### **4. SYSTEM MANAGEMENT**

- 4.1. The system will be administered and managed by the Network Manager who will act as the System Manager, in accordance with the principles and objectives expressed in the policy.
- 4.2. The day-to-day management will be the responsibility of both the Head teacher (Senior Information Risk Officer) and the Business Manager who will act as the System Owner, in accordance with the principles and objectives expressed in the policy.
- 4.3. Use of the system will be limited to those specified in 1.2 above, upon request.
- 4.4. The CCTV system will be operated 24 hours each day, every day of the year.
- 4.5. Data is retained for a period of 30 days.

- 4.6. The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.
- 4.7. 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.
- 4.8. Before accessing the system, those listed in 1.2 above must satisfy themselves of the identity of any person wishing to view images and the legitimacy of the request. Where any doubt exists requests will be refused.
- 4.9. All image/video extractions must be logged. All external requests must be pre-authorised by the Head teacher (or deputy in their absence).
- 4.10. Details of **ANY/ALL** access to the system are recorded electronically in the system log including time/data of access.
- 4.11. The system log will be used to monitor CCTV access by the System Owner-

## 5. LIAISON

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

## 6. DOWNLOAD MEDIA PROCEDURES

- 6.1. In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures:
  - 6.1.1. Each download media must be identified by a unique mark.
  - 6.1.2. All download requests will be logged including its reference, with the date and time of download, authorisation and media used. The log will be held in:  
  
Exchange > Files for others > CCTV Incident Footage > CCTV Download Log
  - 6.1.3. Download media required for evidential purposes must be sealed, witnessed and signed by the System Owner, then dated and stored in a separate secure area. If a download 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 Owner, then dated and returned to the secure area.
  - 6.1.4. If download media is archived (i.e. retained for over 30 days) the reference must be noted.
- 6.2. Images may be viewed by the police for the prevention and detection of crime (at the discretion of the Head teacher).
- 6.3. A record will be maintained of the release of any download media to the police or other authorised applicants.

- 6.4. Viewing of images by the police must be recorded in writing.
- 6.5. 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 download media (and any images contained thereon) remains the property of the school, and download 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 downloaded media this will be produced from the secure evidence store, complete in its sealed bag.
- 6.6. 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 they are needed by the police.
- 6.7. Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the school's legal advisors.

## **7. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE**

- 7.1. Performance monitoring, including random operating checks, may be carried out by the S.I.R.O (Headteacher) or the System Owner.

## **8. COMPLAINTS**

- 8.1. Any complaints in relation to the school's CCTV system should be addressed to the Business Manager.

## **9. ACCESS BY THE DATA SUBJECT**

- 9.1. 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.
- 9.2. Requests for Data Subject Access (Subject Access Request) should be made to the Business Manager. Responding to such requests may take up to 20 days.

## **10. PUBLIC INFORMATION**

- 10.1. Copies of this policy will be available to the public from the school office
- 10.2. A Privacy Notice relating to the use of CCTV within the school can be found on the school website.

## **11. SUMMARY OF KEY POINTS**

- 11.1. This Policy will be reviewed every two years.
- 11.2. The CCTV system is owned and operated by Great Baddow High School.
- 11.3. The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.
- 11.4. Liaison meetings may be held with the police and other bodies if required.
- 11.5. Downloaded media will be used properly indexed, stored securely and destroyed after appropriate use, in accordance with the Data Protection Act.
- 11.6. Images may only be viewed by authorised School staff.
- 11.7. Downloaded media required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.
- 11.8. Downloaded media will not be made available to the media for commercial or entertainment purposes.

## **REFERENCES INFORMATION**

### **Information Commissioners Office (ICO)**

<https://ico.org.uk/for-the-public/>

<https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/>