

QUEEN'S HILL PRIMARY & NURSERY SCHOOL



CCTV Policy



**CCTV is in use for
public safety and
the prevention and
detection of crime and
disorder**

1. INTRODUCTION

- 1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Queen's Hill Primary & Nursery School, hereafter referred to as 'the school'.
- 1.2. The system comprises of seventeen (17) fixed cameras located around the school site. Live and recorded access to the CCTV is provided to authorised user staff only.
- 1.3. This Policy follows Data Protection Act guidelines.
- 1.4. The School Policy will be subject to review annually to include consultation as appropriate with interested parties.

2. OBJECTIVES OF THE CCTV SYSTEM

- 2.1. To protect pupils, staff and visitors.
- 2.2. To provide a safer, more secure environment for pupils and staff and to prevent bullying.
- 2.3. To increase personal safety and reduce the fear of crime.
- 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.
- 2.7. To assist in identifying, apprehending and prosecuting offenders.
- 2.8. To assist in managing the school.

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 to monitor activities within the school and its grounds to identify criminal activity actually occurring, anticipated, or perceived. It will be used for the purpose of securing the safety and well being of the pupils, staff and school together with its visitors.
 - 3.3.1. The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.
- 3.4. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
 - 3.4.1. Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police and in line with the data protection act.

- 3.4.2. Images will never be released to the media for purposes of entertainment.
- 3.5. 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.
- 3.6. 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 Site Manager who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.
- 4.2. The day-to-day management will be the responsibility of the Data controller.
- 4.3. The Head Teacher will act as the System Manager.
- 4.4. The system and the data collected will only be available to the Data Controller and the System Manager.
- 4.5. The CCTV system will be operated 24 hours each day, every day of the year.
- 4.6. The Data controller will check and confirm the efficiency of the system daily 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. The System Manager must be satisfied of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists access will be refused.
- 4.9. Details of **ALL** visits and visitors will be recorded in the system log book including time/data of access and details of images viewed.
- 4.10. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

5. DOWNLOAD MEDIA PROCEDURES

- 5.1. 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: -
 - 5.1.1. Each download media must be identified by a unique mark.
 - 5.1.2. Before use, each download media must be cleaned of any previous recording.

- 5.1.3. The Data controller will register the date and time of download media insertion, including its reference.
- 5.1.4. Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager and the Data controller, then dated and stored in a separate secure evidence store. 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 Manager and the Data controller, then dated and returned to the evidence store.
- 5.1.5. If download media is archived the reference must be noted.
- 5.2. Images may be viewed by the police for the prevention and detection of crime.
- 5.3. A record will be maintained of the release of any download media to the police or other authorised applicants.
- 5.4. Viewing of images by the police must be recorded in writing.
- 5.5. 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 a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.
- 5.6. 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.
- 5.7. Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Boards, Legal department.

6. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

- 6.1. Performance monitoring, including random operating checks, may be carried out by the System Manager or the Data Controller.

7. COMPLAINTS

- 7.1. Any complaints in relation to the school's CCTV system should be addressed to the Head Teacher (System Manager)

8. ACCESS BY THE DATA SUBJECT

- 8.1. 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.
- 8.2. All request should be made in writing to the Head Teacher (System Manager).
- 8.3. Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the school receives a request under the Data Protection Act it will comply with requests within 40 calendar days of receiving the request. The school may charge a fee for the provision of a copy of the images. If the school receives a request under the Freedom of Information Act it will comply with requests within 20 working days of receiving the request. As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely as a Freedom of Information request. Those requesting access must provide enough detail (date, time and location) to allow the operator to identify that they are the subject of the images, and for the operator to locate the images on the system.
- 8.4. Requests for Data Subject Access should be made to the Head Teacher (System Manager).
- 8.5. Refusal to disclose images may be appropriate where its release is:
 - 8.4.1. Likely to cause substantial and unwarranted damage to that individual.
 - 8.4.2. Likely to cause substantial and unwarranted damage to that individual.
 - 8.4.3. Likely to prejudice the legal rights of other individuals or jeopardise an on - going investigation.

9. ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

9.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

10. FEES

10.1 A fee of £15 will be charged per request.**

11. PUBLIC INFORMATION

11.1. Copies of this policy will be available to the public from the school office.

12. SUMMARY OF KEY POINTS

- 12.1. This Policy will be reviewed every year.
- 12.2. The CCTV system is owned and operated by Queen's Hill Primary & Nursery School.
- 12.3. The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.
- 12.4. Liaison meetings may be held with the police and other bodies if required.
- 12.5. Downloaded media will be used properly indexed, stored and destroyed after appropriate use, in accordance with the Data Protection Act.
- 12.6. Images may only be viewed by authorised members of staff and the police.
- 12.7. Downloaded media required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- 12.8. Downloaded media will not be made available to the media for commercial or entertainment purposes.

REFERENCES INFORMATION

The Data Protection Act

http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf

The Commissioners Act

<http://www.legislation.gov.uk/ukpga/1998/29/schedule/11/crossheading/northern-ireland>

** Fees may apply depending on the nature of the request.