ST. BRIGID'S SCHOOL

CLOSED CIRCUIT TELEVISION

(CCTV) POLICY

March 2017

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 St. Brigid's School, hereafter referred to as 'the school'.

1.2. The system comprises of six fixed cameras located in and around the school site. All cameras are monitored from IT office, within the main school building, and images are only available to selected senior staff.

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 protect pupils, staff, governors and visitors.

2.2. To increase personal safety and reduce the fear of crime.

2.3. To protect the school buildings and assets.

2.4. Without prejudice, to protect the personal property of pupils, staff, governors and visitors.

2.5. To support the police in preventing and detecting crime.

2.6. To assist in identifying, apprehending and prosecuting offenders.

2.7. 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 wellbeing of the pupils, staff, governors 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.

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 Business and Finance 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 both the principal and the Facilities Support Officer who will act as the System Manager.

4.3. The system and the data collected will only be available to the Data Controller, the Headteacher and the System Manager.

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

4.5. The System 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.

4.6. 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.

4.7. The System Manager must satisfy themselves 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.

4.8. Details of **ALL** visits and visitors will be recorded in the system log book including time/data of access and details of images viewed.

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

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. Before use, each download media must be cleaned of any previous recording.

6.1.3. The System Manager will register the date and time of download media insertion, including its reference.

6.1.4. Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager, 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, then dated and returned to the evidence store.

6.1.5. If download media is archived the reference must be noted.

6.2. Images may be viewed by the police for the prevention and detection of crime.

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 a 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 Boards, Legal department.

7. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

7.1. Performance monitoring, including random operating checks, may be carried out by the Principal or the Data Controller.

8. BREACHES OF THE CODE (including breaches in security)

8.1. Any breach of this policy by school staff will be initially investigated by the Headteacher (or appointed senior member of staff to this role), in order for them to take the appropriate disciplinary action.

8.2. Any information security breaches will be dealt with in accordance with the 'Information Security Breach Procedure', as published on the school's website.

9. COMPLAINTS

9.1. Any complaints about the schools CCTV system should be in writing, and addressed to the Headteacher or, where the complaint is about the Headteacher, to the Chair of Governors.

9.2. Complaints will be investigated in accordance with this policy. Please, also, refer to school's Complaints Policy, as published on the school's website.

10. ACCESS BY THE DATA SUBJECT

10.1. 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.

10.2. 'Subject Access Requests' should be made in writing, with the appropriate ID, to the Headteacher and the School reserves the right to charge a fee of £10 in accordance with the Act. Digital recordings will be kept for a maximum of 28 days, unless specific incidents have been recorded to disk for investigation..

11. PUBLIC INFORMATION

11.1. Copies of this policy will be available to the public from the school office and will be published on the school's website.

12. SUMMARY OF KEY POINTS

12.1. This Policy will be reviewed every two years.

12.2. The CCTV system is owned and operated by St. Brigid's 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 School 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.

Further Information

Freedom of Information Act 2000

Since January 2005, anyone can request access to any piece of information that the school holds and CCTV falls within the scope of “information held".

By regularly deleting/overwriting your CCTV tapes in accordance with your retention policy, you will reduce the amount of CCTV information held. If the CCTV data is held at the time of a FOI request, you cannot subsequently delete it, even if it falls due for deletion under your retention guidelines. Careful consideration must be given to any release of personal data under the FOIA in order to avoid any breach of the data protection principles.

Employment Practices Data Protection Code – Monitoring Staff at Work

The Information Commissioner has issued a code of practice for employers to follow when monitoring staff. Head Teachers and Governors should be familiar with the requirements of the codes when setting the school’s policy for use of CCTV.

The code can be viewed at

http://www.ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx

Also on the school’s website (www.st-brigids.co.uk)**:**

Publication Scheme
Data Protection Policy
Freedom of Information Policy
Complaints Policy
Fair Processing Notice
Information Security Breach Procedure
Clean Desk / Clear Screen Policy and Procedure