



St. Mary's Grammar School, Belfast

POLICY ON THE USE OF
CCTV

December 2017



CCTV System Policy

1. Introduction

- 1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) system at St Mary's CBGS hereafter referred to as 'the school'.
- 1.2. The system comprises a number of cameras located in and around the school site. All cameras are monitored when required from the office and images are only available to selected senior staff.
- 1.3. This Code follows Data Protection Act guidelines.
- 1.4. The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.
- 1.5. The CCTV system is owned by the School and serviced by Group 4 Security.

2. Objectives of the CCTV system

- 2.1. To protect pupils, staff 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 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 be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and 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, and 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.
 - 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 placed at all access routes to areas covered by the school CCTV system.

4. System Management

- 4.1. The system will be administered and managed by the Principal who will act as the Data Controller, in accordance with the principles and objectives expressed in the code.
- 4.2. The day-to-day management will be the responsibility of both the Senior Leadership Team and the Director of Corporate Services who will act as the System Manager or in his absence the Assistant Director of Corporate Services.
- 4.3. The system and the data collected will only be available to the Data Controller, the Senior Leadership Team and the System Manager. Other staff eg Year Heads, Form Teachers etc, may be asked to view and identify students.
- 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 regularly 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 and the Senior Leadership Team must satisfy themselves of the identity of any person wishing to view images and the legitimacy of the request. Where any doubt exists access will be refused.
- 4.8. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- 4.9. If out of hours emergency maintenance arises, the System Manager must be satisfied of the identity and purpose of contractors before allowing access to the system.

5. Liaison

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

6. Video tape and 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 tape or download media used to record events from the hard drive must be prepared in accordance with the following procedures: -
 - 6.1.1. Each tape or download media must be identified by a unique mark.
 - 6.1.2. Before use, each tape or download media must be cleaned of any previous recording.
 - 6.1.3. The System Manager will register the date and time of tape or download media insertion, including its reference.
 - 6.1.4. A tape or download media required for evidential purposes must be sealed, witnessed, signed by the System Manager, dated and stored in a separate, secure evidence store. If a tape or 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, signed by the System Manager, dated and returned to the evidence store.
 - 6.1.5. If tapes or 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 tapes or download media to the police or other authorised applicants. A register will be available for this purpose.
- 6.4. Viewing of images by the police must be recorded in writing and in the log book.
- 6.5. Should images be required as evidence, a copy may be released to the police under the procedures described in this code. Images will only be released to the police on the clear understanding that the tape or download media (and any images contained thereon) remains the property of the school, and both the tape or 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 tape or download media (and any images contained thereon) to any other person. On occasions when a Court requires the release of an original tape or download 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 stored tapes or download media for possible use as evidence in the future. Such tapes or download media will be properly indexed and properly 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 Principal. In these circumstances tapes or download 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. The following fees can be charged in such circumstances: -
 - 6.7.1. £10 for subject access requests
 - 6.7.2. A sum not exceeding the cost of materials in other cases.

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

- 7.1. Any breach of the Code of Practice by school staff will be initially investigated by the Data Controller, in order for him/her to take the appropriate disciplinary action.
- 7.2. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

8. Assessment of the system and code of practice

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

9. Complaints

- 9.1. Any complaints about the school's CCTV system should be addressed to the Data Controller.

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. Requests for Data Subject Access should be made on an application form available from the Principal.

11. Public information

- 11.1. Copies of this Code of Practice will be available to the public from the school office and the Data Controller.

12. Summary of Key Points

- 12.1. This Code of Practice will be reviewed every two years.
- 12.2. The CCTV system is owned and operated by St. Mary's CBGS.
- 12.3. The CCTV system and images are not available to visitors except by prior arrangement and good reason.
- 12.4. Liaison meetings may be held with the police and other bodies.
- 12.5. Recording tapes or download media will be used properly indexed, stored and destroyed after appropriate use.
- 12.6. Images may only be viewed by authorised school officers and the police.
- 12.7. Tapes or download media required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- 12.8. Tapes or download media will not be made available to the media for commercial or entertainment.
- 12.9. Tapes or download media will be disposed of securely by incineration.
- 12.10. Any covert surveillance being considered or planned as part of an operation should be discussed with the Board of Governors.
- 12.11. Any breaches of this code will be investigated by the Data Controller. An independent investigation will be carried out for serious breaches.
- 12.12. Breaches of the code and remedies will be reported to the Data Controller.

Approvals

- Signatures:

Principal

Chair of Governors

- Date of approval by Governors:

___ / ___ / _____

- Date of next annual review:

___ / ___ / _____