Greenwich Catholic Schools Trust

CCTV POLICY

DATE REVIEWED: **June 2018**
NEXT REVIEW DUE: **September 2019**

1. INTRODUCTION

1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) within The Greenwich Catholic Schools Trust, hereafter referred to as 'the Trust'.

1.2. The system comprises of cameras located in and around sites that are part of the Trust. Cameras are monitored from

St Mary's Catholic Primary School	Reception

1.3. This Policy follows the Trust's Data Protection Policy.

1.4. The Policy will be subject to review annually.

2. OBJECTIVES OF THE CCTV SYSTEM

2.1. To protect students, staff and visitors.

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

2.3. To protect the Trust's buildings and assets.

2.4. Without prejudice, to protect the personal property of students, 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 Trust's schools.

3. STATEMENT OF INTENT

3.1. The CCTV system will seek to comply with the requirements both of Data Protection legislation and the Commissioner's Code of Practice.

3.2. The Trust will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as protected data.

3.3. Cameras will be used to monitor activities within the Trust's schools 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 students, staff and the Trust's sites 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 the 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 Trust sites.

4. SYSTEM MANAGEMENT

4.1. The system will be administered and managed by the Trust 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

St Mary's Catholic Primary School	Premises Manager

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

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

4.5. 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.

4.6. 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.

4.7. Details of **ALL** access to the system will be recorded including time/data of access and details of images viewed.

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 System Manager 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, 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.

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 Trust, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust 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 Trust 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 Trust's legal advisors.

6. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

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

7. COMPLAINTS

7.1. Any complaints in relation to the Trust's CCTV system should be addressed to the Trust's Data Protection Officer (DPO).

8. ACCESS BY THE DATA SUBJECT

8.1. Data Subjects (individuals to whom "personal data" relate) have a right to view data held about themselves, including those obtained by CCTV.

8.2. Details of the access arrangements can be found in the Trust's Data Protection Policy.