The
Pope Francis Catholic
Multi Academy Company

Imago Dei

CCTV POLICY

POLICY INFORMATION SHEET	
Title	CCTV Policy
Source	Unknown
Document Owner	Governance Manager
Approval Level	MAC Estates, Safeguarding and Health and Safety Committee
Date Approved	1 April 2021
Date of Publication on PFMAC Website	
Date of next Review	1 April 2023
Statutory / Non-Statutory	Statutory if CCTV onsite
Required on school websites	Yes

1. INTRODUCTION

1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) across The Pope Francis MAC, hereafter referred to as 'the MAC'.

1.2. The system comprises a number of fixed dome cameras located in and around the MAC site. All cameras are monitored from designated workstations and images are only available to selected staff.

1.3. This Policy follows Data Protection Act guidelines.

1.4. The MAC 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 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. To support the police in preventing and detecting crime.

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

2.6. 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 and school together with its visitors.

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 designated person within the school who will act in accordance with the principles and objectives expressed in the policy.

4.2. The day-to-day management will be the responsibility of the Network Manager who will act as the System Manager.

4.3. The system and the data collected will only be available to the Principal / Headteacher and the System Manager or approved delegates.

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. 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 requests for viewing CCTV using playback will be recorded including time/data of access and details of images viewed, who requested it and the reason.

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 and dated.

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

6.1.3. 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.

6.1.4. 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. A formal written request must be received from the Investigating Officer and records retained.

6.3. A record will be maintained of the release of any download media to the police or other authorised applicants.

6.4. 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.

6.5. 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.

6.6. Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the MACs Legal department (Browne Jackson).

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. COMPLAINTS

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

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. However CCTV will not be shared as part of a Subject Access Request, because in the context of a school the confidentiality of other subjects could not be protected. Where appropriate, data subjects could receive a transcript which narrates events viewed by an appropriate member of staff, delegated by the Principal. Any narration must be redacted to protect the identity of other subjects.

10. PUBLIC INFORMATION

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

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 the School

11.3. The CCTV system and images are not available to visitors

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 and destroyed after appropriate use, in accordance with the Data Protection Act.

11.6. Images may only be viewed by authorised School/staff and the police.

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

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

SCHOOL CCTV designated workstations and selected staff.

Only the following have access to the CCTV, they are permitted to allow other members of staff to view if supervised. Members of the public are not permitted to view video footage.

Students are not permitted to view CCTV.

No member of staff is to download Videos / Pictures unless directed by the Head / Deputy Head. If video / pictures are downloaded this needs to be recorded.

Staff Access

Work station with CCTV access