CCTV

Committee Name:	Full Governing Body
Date of Approval:	May 2018
Validity Date:	2018-2020
Person responsible:	Premises Manager

This school policy is adapted from a model policy drawn up by NEELB. Please note that this policy is written to comply with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018. As such this policy may require some modification once the Act has passed through Parliament.

Contents

1. Introduction
The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at St Fidelis Catholic Primary School hereafter referred to as 'the school'. The system comprises of 24 cameras located in and around the school site. All cameras are monitored from the Network Cupboard and images are only available to selected senior staff.

This Policy follows GDPR guidelines. The School Policy will be subject to review every two years to include consultation as appropriate with interested parties.

2. Objectives
- To protect pupils, staff and visitors.
- To increase personal safety and reduce the fear of crime.
- To protect the school buildings and assets.
- Without prejudice, to protect the personal property of pupils, staff and visitors.
- To support the police in preventing and detecting crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To assist in managing the school.

3. Statement of Intent
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.

The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.

Images will never be released to the media for purposes of entertainment.

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.

Warning signs, as required by the Code of Practice of the Information Commissioner are clearly visible on the site.

4. Legislation and guidance
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information

5. System Management

The system will be administered and managed by the school who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.

The day-to-day management will be the responsibility of both the Headteacher and the Premises Manager who will act as the System Manager.

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

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

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.

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.

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.

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

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

6. Download Media Procedures
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:

Each download media must be identified by a unique mark.

Before use, each download media must be cleaned of any previous recording.
The System Manager will register the date and time of download media insertion, including its reference.

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.

If download media is archived the reference must be noted.

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

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

Viewing of images by the police must be recorded in writing.

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.

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.

Applications received from outside bodies to view or release images will be referred to the local authority's legal department for advice.

7. Assessment of the System and Code of Practice
Performance monitoring, including random operating checks, may be carried out by the Headteacher or the Data Controller.

8. Complaints
Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

9. Access by the Data Subject
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.
Requests for Data Subject Access should be made to the school.