

CCTV Systems And Data Management Policy



"Live as free people"

St Peter's Community School

Approved November 2017

CLOSED CIRCUIT TELEVISION SYSTEMS

A Closed Circuit Television System (CCTV) is installed in St. Peter's Community School under the remit of the Board of Management (BOM).

Purpose of the Policy

The purpose of this policy is to regulate the use of CCTV and its associated technology in the monitoring of the internal and immediate external environs of premises under the remit of the BOM of St. Peter's Community School. All cameras are under the control of the BOM.

Purpose of CCTV Systems

CCTVs are installed internally and externally on the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation to deter bullying, crime, vandalism and theft, as an aid to Health and Safety and to the discharge of the school's duty of care within and/or in the external environs of the premises during both the daylight and night hours each day.

Scope of Policy

This Policy applies to all personnel in and visitors to St. Peter's Community School and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of such recorded material.

General Principles

The BOM of St. Peter's Community School, as the Corporate Body, has a statutory responsibility for the protection of its property, equipment and other plant, as well as providing a sense of security to its employees, students and invitees to its premises. St. Peter's Community School owes a duty of care under the provision of Health, Safety and Welfare legislation and utilises CCTV systems and its associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of St. Peter's Community School by integrating the best practices governing the surveillance of its premises.

The primary aim of CCTV monitoring St. Peter's Community School's premises is to deter crime and vandalism and to assist in the protection and safety of the said property and its associated equipment and materials.

Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited by this policy, e.g. CCTV monitoring of political or religious activities, or employee and/or student evaluations would undermine the acceptability of the resources for use regarding critical safety and security objectives and is therefore prohibited by this policy.

Information obtained through video monitoring may only be released when authorised by the Principal, following consultation with the Chairperson of the Board of Management.

CCTV Monitoring of public areas, for security purposes, will be conducted in a manner consistent with all existing policies adopted by the BOM including the Policy on Bullying and other relevant policies including the provisions set down in equality and other education related legislation.

Video monitoring of public areas, for security purposes, within the said establishment, is limited to uses that do not violate the reasonable expectation to privacy as defined by law.

The Principal will provide written material describing the purpose and location of CCTV monitoring and guidelines for its use. The location of outdoor CCTV cameras will also be indicated to the BOM. Data from the CCTV system will be accessed and used in accordance with Data Protection Regulations.

Fourteen cameras are located in the following internal areas:

- Two cameras in the 'A' corridor (office side)
- Two cameras in the 'A' corridor (library side)
- Two cameras in the General Purpose Area (GPA)
- Two cameras in the 'B' corridor (art room side)
- Three cameras in the 'C' area
- Two cameras in the 'D' area
- One camera in the corridor outside A03/B03 (upstairs)

Signs are erected in each location in which a camera is located. The signs include the name and contact detail of the Data Controller as well as the specific purposes for which the CCTV camera is in place in each location. For example:

- To deter/detect bullying
- To deter/detect crime, theft and vandalism
- To ensure compliance with the schools Code of Behaviour
- As an aid to security
- For Health and Safety purposes
- To enable the school to discharge its duty of care

Staff, students and parent(s)/guardian(s) are informed of the existence and purposes of the CCTV system as outlined above. The right of access for students and staff to images captured by CCTV cameras shall be in accordance with the Data Protection Acts 1998 and 2003 and/or subsequent Data Protection Acts or Amendments as outlined below.

DATA PROTECTION

All personal data recorded and stored by the CCTV system is governed by the Data Protection Acts 1998 and 2003 and/or subsequent Data Protection Acts or Amendments. Under the Data Protection Acts a Data Controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information in manual files or in computerised form. The Data Controller, in respect of images recorded and stored by the CCTV system in the school, is the Principal on behalf of the Board of Management.

The Personal data recorded and stored by the CCTV system will only be available to the Data Controller and will be used only for the purposes outlined on the signage. The CCTV system shall not be used to monitor staff performance or conduct.

Individuals whose images are recorded and stored by the CCTV system shall have the right to request and receive a copy of personal data processed by the system. Such requests shall be made in writing to the Data Controller and shall be complied with within a maximum of forty days. The Data Controller will consult with the Chairperson of the Board of Management prior to the release of any copies of personal data.

Personal data recorded by the CCTV system shall be retained for a maximum of twenty-eight days. Thereafter it will be deleted automatically.

The recorded footage and the monitoring equipment shall be securely stored in the Deputy Principal's office. Unauthorised access to that office is not permitted at any time.

The following procedures shall be followed in the event that An Garda Síochána seek to view or take a copy of CCTV footage from the schools CCTV system:

- 1) The Data Controller shall satisfy himself/herself that there is an investigation underway by telephoning the Garda Station of the requesting Garda and speaking to the Station Sergeant or higher or to a member of the District Office.
- 2) A request from An Garda Síochána must be made in writing on Garda headed notepaper.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the BOM.

Responsibilities

The Principal will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by the BOM
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes with the school
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at St. Peter's Community School is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or material in compliance with this policy
- Maintain a record of the release of discs or any material recorded or stored in the system
- Ensure that material is not duplicated for release, except by an Garda Síochána as specified above
- Ensure that the perimeter view from fixed location cameras conform to this policy both internally and externally

- Provide a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment, located in the school to the Board of Management for formal approval
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. Note: (Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for criminal investigations)
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Advise the BOM to ensure that adequate signage, at appropriate and prominent locations, is displayed and include the following in such signage – ‘THIS AREA IS SUBJECT TO VIDEO MONITORING BY THE SCHOOL MANAGEMENT AUTHORITY’.
- Ensure that external cameras are non-intrusive in terms of their positions and views of residential housing and comply with the principle of ‘Reasonable Expectation of Privacy’
- Ensure that monitors are stored in a secure place with access by authorised personnel only
- Ensure that recorded material is retained for a period not longer than twenty-eight days and will then be erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the BOM
- Ensure that camera control is solely to monitor suspicious behaviour and not individual characteristics
- Ensure that camera control is not in breach of the intrusion on intimate behaviour by persons in public areas
- Ensure that mobile video equipment will only be used for criminal investigations and with the approval of the BOM and the local Garda authorities

DATA MANAGEMENT

Disclosure

- Parental consent will be sought before transfer of student data to the Department of Education & Science. This consent will be sought at the time of enrolment/registration by means of a field on the Enrolment/Registration Form.
- All documents supplied to BOM members containing personal data must be collected and shredded at the end of each meeting.

Data Retention

All documentation containing personal data relating to employees and students must be deleted/shredded when no longer required for business purposes. Employment contracts and superannuation records should only be deleted/shredded on the death of the individual.

Enrolment forms and other personal details relating to students should be deleted/shredded not more than two years after the student has left school.

ICT

All Information Technology (IT) support and maintenance contracts must have clear data protection provision.

Offices

Access to the main office will be restricted to the office staff, the Principal, the Deputy Principal and authorised staff members with the approval of the Principal.