



**St. Mary's Secondary School
Holy Faith Convent
Glasnevin,
Dublin 11**



CCTV Policy

Review Dates:

Staff	7th March 2018	Reviewed
Parents	7th March 2018	Reviewed
Student Council		Reviewed
Board of Management	7th March 2018	Ratified

Due for next review:

Table of Contents

Section	
1. Purpose of the Policy	Page 3
2. Purpose of the CCTV System	
3. Scope of this Policy	
4. General Principles	
5. Justification of Use	Page 4
6. Location of the CCTV Cameras	Page 4
7. Data Protection	Page 5
8. Responsibilities	Page 6
9. Implementation and Review	Page 7
10. Appendix 1: Definitions	Page 8

Mission Statement

St. Mary's follows the Holy Faith philosophy of creating an inclusive school community whose central purpose is the religious, moral, intellectual, human, social and physical-recreational education of the student. The education programme of the school is directed towards the growth of the whole person. It aims to form integrated and self-reliant people who are eager to build a better world.

1. 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 environs of the school premises.

2. Purpose of the CCTV System

The CCTV system is installed internally and externally in premises for the purpose of enhancing security and protection 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 during the day light and night hours, 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 at all times.

3. Scope of this policy

This applies to all personnel in and visitors to St Mary's Secondary School, Glasnevin, Dublin 11. It relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of such recorded material.

4. General Principles

The Board of Management has a statutory responsibility for the protection of the school property and equipment as well as providing a sense of security to its employees, students and invitees to its premises. The 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 in the school by integrating the best practices governing the surveillance of its premises.

The primary aim of the CCTV monitoring of the school 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. For example, 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 the CCTV system 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 the Code of Behaviour, the Anti-Bullying Policy and all other existing policies adopted by the Board of Management including the provisions set down in Equality and other Education related legislation.

The industry code of practice for video monitoring prohibits monitoring based on the classifications contained in Equality and other related legislation e.g. gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of the Traveller community.

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

Data from the CCTV system will be accessed and used in accordance with Data Protection Regulations.

5. Justification of Use of CCTV

The use of CCTV to control the perimeter of the school buildings for security purposes has been deemed to be justified by the Board of Management. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, the Principal has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

6. Cameras are located in the following areas:

Internal Cameras	Floor
1. Admin Office	1
2. Room 11 – basement	0
3. Bottom corridor towards staff room	1
4. Bottom corridor towards reception	1
5. Middle corridor towards food station	3
6. Middle corridor towards room 27/28	3
7. Top corridor towards room 35	5
8. Top corridor towards computer room	5

External Cameras

12. Staff entrance - courtyard
13. Car park – view towards Gym
14. Car park
15. St. Anne’s kitchen towards Botanic Gardens
16. Staff room – towards St. Anne’s kitchen
17. Tennis Courts towards Convent
18. Tennis Courts towards grounds
19. Glass passage from Library
20. Glass passage from Offices
21. Gym and student entrance
22. Gym and outside lab.

Signage will be erected in locations throughout the school.

Staff, students and parents/guardians will be informed of the location and purpose of the CCTV system as outlined above. The right to access images captured by CCTV cameras shall be in accordance with the Data Protection Acts of 1998 and 2003. St Mary’s Secondary School has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.

7. Data Protection

All personal data recorded and stored by the CCTV system is governed by the Data Protection Acts of 1998 and 2003. 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 a 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.

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 40 days. Where there are images of other students/personnel in the data requested these may need to be pixelated and redacted. Personal data recorded by the CCTV system shall be retained for a maximum of 28 days. Thereafter it will be deleted automatically.

The recorded footage and the monitoring equipment shall be securely stored in the office area. Unauthorised access to that office is not permitted at any time. The office is locked when not occupied.

The following procedures shall be followed in the event that An Garda Síochána seeks to view or take a copy of CCTV footage from the school's CCTV systems:

1. The data controller shall satisfy himself/herself that there is an investigation underway.
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.

8. Responsibilities:

The Board of Management will:

- Ensure that a policy is in place, compliant with relevant legislation, to govern the use of CCTV in the school.
- Ensure this policy is reviewed regularly by the Board of Management.

The following personnel have access to the CCTV System: The Principal and the two Deputy Principals, and admin personnel on a need to know basis.

The Principal will:

- Act as Data Controller on behalf of the Board of Management.
- Ensure that the use of the CCTV system is used in accordance with the policy set down by the Board of Management.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the school.
- Ensure that all CCTV monitoring systems are compliant with this policy.
- Be responsible for the release of any information or material in compliance with this policy.
- Maintain a record of the release of any material recorded or stored on this system.
- Provide a list of the CCTV cameras, their locations and the associated monitoring equipment and the capabilities of such equipment 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.
- Ensure that all areas being monitored are not in breach of a reasonable expectation of the privacy of individuals within the school.
- Advise the Board of Management to ensure that adequate signage, at appropriate and prominent locations, is displayed.
- Ensure that external cameras are not intrusive in terms of their positions and views of residential housing and comply with the principle of "***reasonable expectation of privacy***".

- Ensure that recorded material is retained for a period not longer than 28 days and will 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 Board of Management.
- Ensure that monitors are stored in a secure place with access by authorised personnel only.

9. IMPLEMENTATION & REVIEW

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, Department of Education and Skills, Audit units (internal and external to the school), national management bodies, legislation and feedback from parents/guardians, students, staff and others.

The date from which the policy will apply is the date of adoption by the Board of Management. Implementation of the policy will be monitored by the Principal of the school.

Policy adopted by the Board of Management



Signed: _____
Chairperson, Board of Management

Date: 7th March 2018

APPENDIX 1 - DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school/ETB staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

