CCTV Policy St. Mary's NS, Knockbridge

Introduction
Closed Circuit Television Systems (CCTVS) are installed in St. Mary's NS and their operation will be reviewed regularly in consultation with staff and the Board of Management.

1. Purpose

The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of the external environs of the premises under the remit of St. Mary's NS.

CCTV systems are installed 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 within the school grounds during both the daylight and night hours each day.
CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, pupils and visitors;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Gardaí in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders;
- ensuring that the school rules are respected in accordance with the school Code of Behaviour so that the school can be properly managed.

2. Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material.

3. General Principles

The Board of Management of St. Mary's NS as the corporate body has a statutory responsibility for the protection of its property and equipment as well providing a sense of security to its employees, students and invitees to its premises. St. Mary's NS has a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

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. Any requests for CCTV recordings/images from An Garda Síochána will be fully recorded and, if necessary, legal advice will be sought. (See 'Access').

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school and other relevant policies, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within school premises is limited to uses that do not violate the individual's expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee or pupil of the school. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the St. Mary's NS. Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003.

4. Justification fo use of CCTV

Section 2(1)(c)(iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that St. Mary's NS needs to be able to justify the obtaining and use of personal data by means of a CCTV system. 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.

5. Location of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. St. Mary's NS has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property. 8 external cameras are fitted around the school grounds covering all 4 entrances, the field, the yard, the boiler house and the staff car park.

6. Notification - Signage

The Principal will provide a copy of this CCTV Policy on request to staff, parents and visitors to the school and on the school website. This policy describes the purpose and location of CCTV monitoring. The location of CCTV cameras will also be indicated to the Board of Management. Adequate signage will be placed at/near each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrances to St. Mary's NS.

WARNING CCTV

Cameras in Operation

Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, for the safety of our staff and students and for the protection of St. Marys NS and its property. This system will be in operation 24 hours a day, every day. These images may be passed to An Garda Síochána. This scheme is controlled by St. Marys NS.

For more information contact 042-9374443.

7. Storage & Retention

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with an automatic log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Principal. The Principal may delegate the administration of the CCTV System to another staff member. In certain circumstances and with the consent of the Board of Management, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Gardai, the Deputy Principal, members of the teaching staff, representatives of the Department of Education and Skills, representatives of the HSE and/or the parent of a recorded student). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

The CCTV system hard disk will be stored in the Principal's office in a secure environment with automatic logs of access to the images created. Access will be restricted to authorised personnel.

8. Access

The CCTV system hard disk storing the recorded footage and the monitoring equipment will be securely stored in a restricted area (Principal's Office). Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. Automatic logs of access to the images created will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Principal of school.
In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána where St. Mary's NS Board of Management are required by law to make a report regarding the commission of a suspected crime;
- Following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on St. Mary's NS property
- To the HSE and/or any other statutory body charged with child safeguarding;
- To assist the Principal in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed;
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to St. Mary's NS
- To individuals (or their legal representatives) subject to a court order.
- To the school's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Requests by An Garda Síochána: Information obtained through video monitoring will only be released when authorised by the Principal following consultation with the Chairperson of the Board of Management. If An Garda Síochána request CCTV images for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be made in writing.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the school Principal. The school may charge up to €6.35 for responding to such a request and must respond within 40 days.

Access requests can be made to the following: The Principal, St. Mary's NS, Knockbridge, Dundalk, County Louth. Eircode A91X330.

A person should provide all the necessary information to assist St. Mary's NS in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school.

9. Responsibilites

The Principal will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by St. Mary's NS.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within St. Mary's NS.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at St. Mary's NS is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to any material recorded or stored in the system
- Ensure that monitoring hard disk coverage is not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy
- 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
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring hard drive is stored in a secure place with access by authorised personnel only
- Ensure that images recorded on digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chairperson of the Board.

- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas

10. 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, 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/Deputy Principal of the school.

Ratification of Policy

This policy was adopted by the Board of Management on **7th November 2019**

Signed: *Helen King*
Chairperson of Board of Management

Signed: *Brian McDonnell*
Secretary of Board of Management

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.