



## **Mary Field College CCTV POLICY**

### **INTRODUCTION**

Closed Circuit Television Systems (CCTVS) are installed in Maryfield College

Their operation will be reviewed regularly by the Board of Management in consultation with staff, students and the parents association.

#### **1. PURPOSE OF POLICY**

“The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Maryfield College.

CCTV systems are installed (both internally and externally) in 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 and in the external environs of the premises 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;**
- ☒ **preventing bullying;**
- ☒ **reducing the incidence of crime and anti-social behaviour (including theft and vandalism);**
- ☒ **supporting the Gardai in a bid to deter and detect crime;**
- ☒ **ensuring that the school rules are respected 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**

Maryfield College Board of Management as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. The Board of Management of Maryfield College

owes 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 legal advice will be sought if any such request is made. (See "Access" below). If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be requested in writing and the school will immediately seek legal advice.

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 reasonable expectation to privacy.

Information obtained may be used to assist school management in the implementation of the School Anti- Bullying Policy and the School Code of Behaviour.. In this regard parents of the student/s concerned will be informed.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by Maryfield College. 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 FOR 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 Maryfield College 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.

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

## **5. LOCATION OF CAMERAS**

Maryfield College has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in Maryfield College may include the following:

- Protection of school buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- Criminal Investigations (carried out by An Garda Síochána): Robbery, burglary and theft surveillance

## **6. COVERT SURVEILLANCE**

Maryfield College will not engage in covert surveillance. Where An Garda Síochána requests to carry out covert surveillance on school premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by An Garda Síochána will be requested in writing and the school will seek legal advice.

## **7. NOTIFICATION – SIGNAGE**

A copy of this CCTV Policy will be provided on request to staff, students, parents and visitors to the school. This policy describes the purpose and location of CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Board of Management. Adequate signage will be placed at 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 entrance to Maryfield College property. The Data Controller is the School Authority Mary Field College Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

### **WARNING**

**CCTV cameras in operation**

**Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of Maryfield College 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 Maryfield College and operated by Integral Security**

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates
- reception area
- at or close to each internal camera

## **8. 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, while many systems have the ability to retain data for longer than 30 days, it would be difficult to justify retention beyond a month (30 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.

Access to control of the system 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, 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, the relevant Year Head, other 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.

Tapes/DVDs/USB will be stored in a secure environment with a log of access to tapes kept.

Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

## **9. ACCESS**

Devices storing the recorded footage and the monitoring equipment of one system will be securely stored in the Principals Office (original system) and in the General Office (additional internal system). Unauthorised access to the recording equipment will not be permitted. 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 Maryfield College (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- ☐ 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 Maryfield College property, or
- ☐ To the HSE and/or any other statutory body charged with child safeguarding; or
- ☐ To assist the Principal in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or
- ☐ To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to Maryfield College, or
- ☐ To individuals (or their legal representatives) subject to a court order.
- ☐ To the schools 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 and the school should immediately seek legal advice.

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 Secretary of the Board of Management. The school may charge up to €6.35 for responding to such a request and must respond within 40 days.

A person should provide all the necessary information to assist Maryfield College 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.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

## 10. RESPONSIBILITIES

The Board of Management has a responsibility to:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Maryfield College
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Maryfield College
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Maryfield College 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 or the release of tapes or any material recorded or stored in the system
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- 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 tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings or other bona fide use as approved by the Chairperson of the Board of Management
- 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

- Ensure that where An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chairperson of the Board.

## **11. SECURITY COMPANIES**

The school external CCTV system is monitored by a security company contracted by the school:

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients). Sections 2(2) and 2C of the Data Protection Acts place a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company has been made aware of their obligations relating to the security of data.

## **12. 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.

The Policy was ratified by The Board of Management on November 27<sup>th</sup> 2017

It will be reviewed annually and in line with any relevant legislation