Policy Title:	CCTV Policy
Description:	Policy outlining the use of CCTV at Marino Institute of Education
Author (Position):	DPO
Version:	1
Approved By:	Governing Body
Policy Approval Date:	June 2021
Date of Next Policy Review:	June 2024 (or as necessary)

Marino Institute of Education CCTV Policy

1. Introduction

This Policy details the accepted uses and management of the Closed Circuit Television Systems (CCTV) of Marino Institute of Education (MIE). CCTV are installed on the premises under the control of MIE to provide for the protection, safety and security of all staff, students and contractors of MIE and of all visitors to the Institute's property. MIE, as a data controller, processes the personal data of individuals through its use if CCTV on its campus at Griffith Avenue, D09 R232.

It should be noted that this policy does not include CCTV cameras situated at the Westcourt student accommodation, which is located on the MIE campus.

Recognisable images captured by CCTV systems are personal data and are therefore subject to the provisions of the, General Data Protection Regulation (GDPR) EU 2016/679, Data Protection Directive 95/46/EC, [hereafter referred to as "data protection legislation"].

Personal Data is defined under Article 4 of the EU General Protection Regulation ('GDPR') as

"*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Day to day responsibility for the College's CCTV system and the data generated rests with the Head of Conferencing and Facilities.

All CCTV Footage is the property of MIE.

2. Policy

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The purpose of this policy is to regulate the use of CCTV in the monitoring of both the internal and external environs of the MIE campus.

The aim is to ensure that CCTV is used transparently and proportionately in accordance with data protection legislation, the Institute's Data Protection Policy and guidance provided by the Data Protection Commission.

CCTV systems are installed (both internally and externally) on the MIE campus ('the Premises') for the purpose of enhancing the security of the campus and buildings, and its associated equipment, as well as creating a mindfulness among the occupants of the Premises that a surveillance security system is in operation within and/or in the external environs of the Premises both during and after normal business hours each day.

3. Scope

CCTV surveillance on the campus is intended for the purposes of:

- protecting MIE buildings and assets, both during and after normal business hours, the Premises' perimeter, entrances and exits, lobbies and corridors, special storage areas;
- promoting and protecting the health and safety of staff and visitors at the premises;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Gardaí in a bid to deter and detect crime;
- providing assistance in criminal investigations (carried out by An Garda Síochána), including robbery, burglary and theft surveillance;
- monitoring of access control systems to monitor and record restricted access areas at entrances to the Premises and other areas;
- verification of security alarms: intruder alarms, exit door controls, external alarms;
- managing any health and safety risks and/or accidents in accordance with the MIE's health and safety obligations and relevant insurance policies.

4. General Principles

MIE has a statutory responsibility to protect its property, equipment and other plant as well as to provide a sense of security to its staff, students, and contractors, and to visitors to its Premises. MIE has a duty of care to such staff, students, contractors, and visitors to its

Premises under the provisions of the Safety, Health and Welfare at Work Act 2005 and associated legislation, and utilises the CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance to assist in meeting such duties. MIE's use of the CCTV system is conducted by the Institute in a professional, ethical and legal manner and utilised for the purpose only. Any deviation from this policy and the use of CCTV for other purposes is prohibited by this policy, eg CCTV will not be used by MIE for monitoring staff or student performance.

Recorded Data obtained by MIE through the CCTV system may only be released by the Head of Conferencing and Facilities as authorised by the DPO through the formal data access request procedures. In the event of an appeal, the President's decision will be final.

Requests must be made in writing using the appropriate forms no more than 10 days after the date being requested. Any requests received by MIE from third parties/data subjects, including from An Garda Síochána for Recorded Data recorded using the Institutes CCTV system, will be appropriately logged by MIE. Legal advice as to MIE's obligations to comply with such request and related matters may be sought at the discretion of the President or their nominee. CCTV monitoring of public areas within or adjacent to the Premises by MIE for security purposes will be conducted in a manner consistent with all relevant policies adopted by MIE and in force at that time.

5. Justification for use of CCTV

Article 5 (b) of the GDPR states that Personal Data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".

This means that MIE needs to be able to justify the obtaining and use of Personal Data by means of CCTV. The use by MIE of CCTV to monitor the Premises for the Purpose outlined has been deemed to be justified by the Institute's management. The CCTV system is intended to capture images of intruders, or of individuals damaging property or removing goods without authorisation and for security, and health and safety purposes.

6. Location of cameras

Article 5 (a) of the GDPR states that Personal Data shall be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*".

The location of the CCTV cameras at the Premises is a key consideration for MIE when operating CCTV. MIE does not seek to locate CCTV cameras to monitor areas of the Premises where individuals would have a reasonable expectation of privacy. MIE has endeavoured to select locations for the installation of CCTV cameras which minimise such intrusion so as to protect the privacy of individuals at the Premises as far as is reasonable. Cameras placed by MIE so as to record external areas of the Premises are, so far as is reasonably possible, positioned to prevent or minimise recording of passers-by or of another person's private property.

7. Notification – signage

A copy of this CCTV Policy will be made available on the MIE website. This policy describes the purpose of CCTV monitoring and provides a contact number for those wishing to discuss the Institute's use of CCTV monitoring, and guidelines for its use with the Institute.

Signage will be placed at locations where CCTV is in operation and also at the entrance to the Institute. Signage shall include the contact details of the Data Controller, dpo@mie.ie, and state the specific purpose(s) for which the CCTV camera is in place in each location at MIE.

Appropriate locations for signage will include:

- at entrances to the Institute, eg main gates, external doors;
- Reception area;
- at or close to each internal camera.

8. Storage and Retention

Article 5 (e) of the GDPR states that Personal Data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*".

All Recorded Data captured by MIE CCTV system will be retained by the Institute for a maximum of 30 days, except where MIE reasonably believes that an image (or images) of such recorded data identifies an issue or potential issue and is retained by MIE specifically in the context of an investigation/prosecution of that issue or potential issue.

Article 5 (f) of the GDPR states that Personal Data shall be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".

All Recorded Data will be stored by MIE in a secure environment and the Institute will maintain an access log recording all individuals accessing such recorded data. Access to recorded data will be restricted by MIE to personnel authorised to access such recorded data ('Authorised Personnel'). Supervising the access and maintenance by MIE of CCTV is the responsibility of the Institute's Head of Conferencing and Facilities.

9. Access

9.1 Requests by Third Parties

MIE shall ensure that hard drives storing the Recorded Data and the monitoring equipment comprising the CCTV system and the system for storing such Recorded Data will be securely stored in a restricted area (the 'Secure Area'). MIE shall endeavour to prevent unauthorised access to the secure area at any time. The Secure Area will be locked when not occupied by the Authorised Personnel. The Institute will maintain an access log recording appropriate details in relation to each access to the Secure Area and viewing of the Recorded Data whether by the Authorised Personnel or any Additional Authorised Individuals.

MIE shall restrict access to the CCTV system and Recorded Data to Authorised Personnel. Where necessary, CCTV footage and Recorded Data deemed may be accessed by Additional Authorised Individuals as follows:

- by An Garda Síochána where MIE 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 or around the campus; or
- by individuals (or their legal representatives) subject to a court order being made obliging MIE to allow access; or
- by MIE's insurers, where the insurers require same in order to pursue a claim for damage done to the Premises or in respect of any health and safety issue occurring or alleged to have occurred at the Premises.

9.2 Access requests by Data Subject

On written request using the appropriate form no more than 10 days after the date being requested, any individual who is the subject of Personal Data (Data Subject) and whose image has been recorded in the Recorded Data has a right to be given a copy of the Recorded Data retained at that time by MIE which relates to him/her, provided always that such Recorded Data exists at the time of the relevant request, ie has not been deleted and provided also that an exemption/prohibition does not apply to the release of such Recorded Data. Where the relevant Recorded Data identifies another individual, that Recorded Data may only be released by the Institute to the Data Subject where the relevant image(s) in the relevant Recorded Data can reasonably be redacted/anonymised/pixelated so that any other person(s) are not identified or identifiable or where the other person(s) have provided his/her explicit consent to the release of the Recorded Data to the Data Subject. To exercise their right of access to Recorded Data relating to a Data Subject, that Data Subject must make an application in writing to the Head of Conferencing and Facilities (a 'Request'), and MIE must respond within one month of receipt of each such Request.
A Data Subject delivering a Request to MIE should provide all information with that Request which the Institute deems necessary in order to assist in locating the requested Recorded Data, such as the date, time and location of the relevant Recorded Data. In the case of the relevant image(s) comprising the Recorded Data being of such poor quality as not to clearly identify an individual, the image(s) may be deemed by MIE to not be Personal Data, may inform the relevant Data Subject who has made the relevant Request of that finding and may decline to hand over the relevant Recorded Data on that basis.

In circumstances where Recorded Data that is the subject of a Request cannot be copied to another device, or in other exceptional circumstances, MIE will endeavour to provide stills of the relevant Recorded Data as alternative to video footage to the Data Subject. All queries should be addressed to the Data Protection Officer at dpo@mie.ie.

9.3 Requests by An Garda Síochána

Information to include Recorded Data obtained by MIE through CCTV will only be released to An Garda Síochána when authorised by the Head of Conferencing and Facilities or another member of staff as delegated by Head of Conferencing and Facilities. If a law enforcement authority, such as An Garda Síochána, is seeking Recorded Data for a specific investigation, such requests are made to the Data Protection Officer at dpo@mie.ie. MIE will seek that any such request is made in writing stating that An Garda Síochána is investigating a criminal matter. MIE may again, at its discretion, seek legal advice on any such requests made by An Garda Síochána. The Data Protection Commissioner's guidance on the use of CCTV makes a distinction between a request by An Garda Síochána to view Recorded Data on the Premises and a request to take away or download a copy of the Recorded Data. MIE will always seek confirmation in writing from An Garda Síochána in respect of a request to take away or download Recorded Data and seek that the written request is on An Garda Síochána headed paper and sets out the details of the Recorded Data required and the legal basis for such a request. In urgent matters, verbal requests from An Garda Síochána to view or access Recorded Data can be dealt with by MIE and can then be followed up by a written request from An Garda Síochána.

MIE does not engage in covert surveillance. Where An Garda Síochána requests the Institute to carry out covert surveillance on the Premises, such covert surveillance must be requested by An Garda Síochána in writing and approved in advance to the Head of Conferencing and Facilities and referred to the President or Vice-Presidents for approval. MIE may seek legal advice in relation to any such request(s) and act accordingly.

9. Responsibility

This Policy is the responsibility of the Head of Conferencing and Facilities in consultation with the Data Protection Officer.

Where evidence shows that a CCTV camera location is no longer justified, the camera shall be removed at the request of the Head of Conferencing and Facilities and placed in storage until required.

Requests for the installation of additional cameras in the Institute shall be made in writing by a member of the Leadership Team to the Head of Conferencing and Facilities. A Data Protection Impact Assessment (DPIA) may be carried out by the applicant in consultation with the DPO using the MIE DPIA Template. The DPIA will require the applicant to substantiate why the privacy rights of individuals must cede, in a proportionate way, to achieve a legitimate objective. Approval, in consultation with the Head of Conferencing and Facilities, will depend on a proven need, taking into account whether better solutions exist and the benefits to be gained from the additional cameras

12. Implementation and Review

The policy will be reviewed and evaluated at least annually by the Head of Conferencing and Facilities. Ongoing review and evaluation will take cognisance of changing legislation, information or guidelines (eg from the Data Protection Commissioner, An Garda Síochána).

13. Related Documents

13.1 MIE Data Protection Policy and Procedures

13.2 MIE Privacy Statement

13.3 MIE Data Subject Access Request Policy