POLICY:		Data Protection Policy

ADOPTED:		Approved UR 2019#01

AMENDMENTS:		First adopted BR 2013#02, amended ET 2018#09

REVIEW:		March 2024

MIC Data Protection Policy

1. **Policy Statement**

Mary Immaculate College (MIC) is committed to the protection of personal data it collects and processes in respect of data subjects, including all students, staff (permanent and temporary) and other individuals who come into contact with the College). EU legislation, which includes the General Data Protection Regulation and the Law Enforcement Data Protection Directive, and the related Irish legislation, being the Data Protection Acts 1988 to 2018 (together, "Data Protection Legislation"), lays down rules about the way in which personal data should be collected, processed and disclosed and how the privacy rights of individuals should be upheld. MIC seeks to fully comply with its obligations under Data Protection Legislation. The College has put in place a range of systems and procedures, which it reviews on a regular basis, in order to protect these rights.

This policy applies to all staff (permanent and temporary), contractors, service providers, and third parties that access, use, store or process information on behalf of MIC. It also applies to any student of MIC who processes personal data in the course of their studies.

2. **What is Data Protection?**

Data protection is the safeguarding of the privacy rights and freedoms of individuals in relation to the collection, processing, storage and retention of their personal data, in both paper and electronic format. A list of definitions related to data protection is attached in Appendix 1. Personal data is defined 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.

3. **Purpose of the Policy**

The purpose of this policy is to set out the personal data protection principles and MIC's approach to fulfilling its compliance obligations concerning the protection of personal data. In order to carry out its core functions, MIC needs to collect and process personal data in respect of its staff, students and other individuals who come into contact with the College. Core functions include the organisation and administration of courses, the conducting of examinations, pursuit of research activities, recruitment and payment of staff, compliance with statutory obligations, etc. MIC is legally obliged to safeguard the privacy rights of individuals in relation

to the processing of their personal data for such purposes. This policy aims to support MIC in:

- Maintaining compliance with Data Protection Legislation
- Protecting the rights of students, staff and all other data subjects in respect of which MIC holds personal data
- Mitigating the risk of a data breach
- Being transparent about how it processes personal data
- Ensuring that appropriate organisational measures are in place to support MIC in managing its legislative obligations, including the appointment of a Data Protection Officer (DPO), and providing clarity regarding the responsibilities of staff and management.

4. Data Protection Principles

MIC undertakes to perform its responsibilities under the legislation in accordance with the key data protection principles set out below:

i. MIC is accountable for the personal data it collects and processes

MIC is responsible for keeping a record of the personal data it processes and must demonstrate compliance with Data Protection Legislation. Compliance may be demonstrated by MIC's implementation of data protection procedures, guidelines and tools including the following:

- Subject Rights Request Procedure
- Records Retention Schedule
- Student and Staff Privacy Notices
- Data Protection Training
- Personal Data Handling Guidelines
- Data Breach Protocol
- CCTV Policy
- Data Protection Impact Assessment Procedure
- Safeguarding Policy

ii. Personal data is processed in a lawful, fair and transparent manner

MIC is responsible for obtaining and processing personal data fairly, transparently, and in accordance with its legal obligations. Transparency is achieved by informing data subjects of the use of their data, how long the data is retained and with whom it may be shared. Data

subjects are informed by way of a privacy notice when personal data is obtained from them or other sources, as appropriate.

In order to collect and process personal data "lawfully", MIC must have a legal basis for doing so and this must be documented in its data protection notices. The six available legal bases for processing, which are set out in Article 6(1) of the GDPR, are as follows:

- **Consent**: the individual has given clear consent for MIC to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract MIC has with the individual, or because they have asked MIC to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for MIC to comply with the law.
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for MIC to perform a task in the public interest or for its official functions.
- **Legitimate interests**: the processing is necessary for the legitimate interests of MIC or a third party.

iii. Personal data is collected for specified, explicit and legitimate purposes

MIC collects personal data for specified, explicit and legitimate purposes only. Personal data may not be processed for a purpose other than that for which it was initially collected, unless the data subject consents, a specific legal basis for relevant processing exists or where the processing for another purpose is compatible with the purpose for which the personal data was initially collected.

iv. Use of personal data is minimised

MIC adheres to a data minimisation principle and does not process personal data unless considered necessary. MIC only uses and discloses personal data in circumstances that are necessary for the purposes for which it collects and keeps the data.

v. Personal data held by MIC is accurate and up-to-date

Each Department of MIC has a responsibility to keep any personal data collected or held, accurate and, where necessary, up to date, taking into account the purpose of processing.

vi. Personal data is retained for no longer than is necessary for the purpose or purposes for which it is collected

MIC has a Records Retention Schedule setting out retention periods for personal data held. Each Department in MIC is required to ensure that personal data is not retained any longer than is necessary and in accordance with the defined retention schedules.

vii. Personal data is secured and its confidentiality is safeguarded

MIC processes data securely and confidentially. This principle applies to IT systems, paper records and as well as ensuring the physical security of data. Where personal data is held electronically, MIC's Information Security policies must be complied with, including the appropriate protection of all relevant files where personal data is held.

5. Risk-based Approach to Compliance

MIC employs a risk-based approach to data protection in order to provide for a proportionate response to its obligations under the Data Protection Legislation. Described below are the various organisational and technological measures applied by MIC to implement the policy statement and principles.

5.1. Data Protection Impact Assessments (DPIAs)

DPIAs are completed for all new projects or initiatives which involve the processing of personal data, which is likely to result in a high risk to the rights and freedoms of individuals.

5.2.Data Security and Handling

MIC uses appropriate organisational and technological measures to keep personal data secure and protect it against loss or misuse at all times. If third parties are processing personal data on behalf of MIC, MIC will establish what, if any, specific data security arrangements need to be specified in Data Protection Agreements with those third parties. The College must protect personal data from unauthorised access when in use and in storage and such data must be protected from inadvertent destruction, amendment or corruption.

- Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, access logs, backup, etc.
- Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.

- Personal manual data including exam scripts must be held securely in locked cabinets, locked rooms or rooms with limited access.
- Subject to the MIC Records Retention Schedule, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PC, ensure the hard drive is cleaned by an appropriate IT staff member.
- Special care must be taken where laptops and PCs containing personal data are used outside the College.
- Special care must be taken to ensure the safety and security of any personal data held on mobile storage media.
- Health and social work personal data can only be released following consultation with the relevant professional.
- Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

5.3. Subject Rights Request

The Data Protection Legislation provides for individual data subjects to have rights to request and control use of their personal data. Data subjects (e.g. staff members and students) have a right to be informed by MIC if it is processing any personal data that relates to them. MIC adopts procedures to ensure it complies with data subjects' rights under Data Protection Legislation to access, edit or erase their personal data.

5.4.Breach of Personal Data

MIC's Personal Data Breach Protocol supports the departments of MIC in reporting and managing breaches in accordance with Data Protection Legislation. All breaches, and potential data protection breaches, must be reported to the DPO as soon as possible.

6. Roles & Responsibilities

As a Data Controller of personal data, MIC has responsibility for ensuring compliance with Data Protection legislation. The Governing Body of MIC has overall responsibility for this policy and for reviewing the extent to which MIC has implemented effective measures to maintain compliance with Data Protection Legislation. Each staff member (permanent and temporary) student, contractor, service provider and third party that accesses, uses, stores or processes information on behalf of MIC must comply with this policy, and adhere to the obligations provided for under MIC's

The Information Compliance Office monitors compliance with Data Protection Legislation and provides support, assistance, advice and training to staff in all

departments and offices in fulfilling compliance with this policy the Data Protection Legislation. The office has responsibility for coordination and compliance relating to all data protection matters, including responding to general queries and requests by Data Subjects relating to personal data as well as requests for assistance from MIC staff members involved in collecting, storing and processing personal information. The office is also responsible for engagement with the Data Protection Commissioner, for processing and responding to subject rights requests and for dealing with data protection breaches.

7. Personal Data Handling Guidelines

There are clear procedures in place at MIC for the collection, processing and maintenance of personal information required by the College to carry out its core functions. This policy is supplemented by the MIC Personal Data Handling Guidelines. This document sets out guidelines in order to raise general awareness of the systems that are in place and also to assist MIC employees to comply with the MIC's Data Protection Policy and the relevant legislation.

The Personal Data Handling Guidelines are available on request from the Information Compliance Office or *dataprotection@mic.ul.ie*.

Queries:

Any queries relating to data protection issues, including requests by individuals for access to and/or correction of any personal data held by the College and relating to such individuals should be directed as follows:

Information Compliance Office
Mary Immaculate College,
South Circular Road,
Limerick
Tel: *+353-61-204511*
E-mail: *dataprotection@mic.ul.ie*

Next Review

This Policy will be reviewed at 5-year intervals in line with MIC protocols. The Policy may be reviewed between such intervals in the event of any legislative change or other developments relevant to MIC's obligations.

Appendix 1: Definitions

Data Controller: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

Data Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Personal Data: means 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;

Special categories of Personal Data: Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "special categories" of personal data. The special categories are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. Processing of these special categories is prohibited, except in limited circumstances set out in Article 9.

Data Subject: a natural person whose personal data is processed by a controller or processor.

Data Protection Impact Assessment (DPIA): a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR.

Appendix 2: Additional MIC Policies within the Data Protection Framework

The following documents have been developed to support this policy and form part of MIC's data protection policy framework:

- Records Retention Schedule
- Privacy Notices
- Personal Data Breach Protocol
- Personal Data Handling Guidelines
- Subject Rights Request Procedures
- CCTV Policy
- Policy for Responsible Computing
- MIC Research Ethics Committee (MIREC) policies and procedures
- Safeguarding Policy
- Procedures for Complaints by a Student
- MIC Text Alert Service Protocol

Implementation of these policies and guidelines will be further supported through training.