Data Protection

1. Policy Statement

Mary Immaculate College (MIC) is committed to protecting the fundamental rights and freedoms of individuals, particularly their right to the protection of personal data. This policy sets out MIC's institutional position and commitment in relation to compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR), the Data Protection Acts 1988–2018, and all other applicable Irish and European Union data protection legislation (together, the Data Protection Legislation).

MIC, as a Data Controller, acknowledges its accountability obligations under Article 5(2) GDPR and is committed to implementing appropriate technical and organisational measures to ensure and demonstrate compliance with data protection requirements. This policy establishes the principles and governance framework that guide how personal data is processed across the College.

2. Scope

This policy applies to:

- All MIC staff, including permanent, temporary and agency staff.
- Members of the Governing Authority and its committees.
- Students, where personal data is processed during their studies.
- Contractors, service providers and third parties who process personal data on behalf of MIC.

3. Related Documents

Legislation

- General Data Protection Regulation (EU) 2016/679
- Data Protection Acts 1988–2018
- Freedom of Information Act 2014 (as amended)
- Universities Act 1997
- Higher Education Authority Act 2022

MIC Policies, Procedures and Supporting Documents

- Subject Rights Request Procedures
- Records Retention Schedule
- Privacy Notices (Staff, Student and Other)
- Personal Data Breach Protocol
- Personal Data Handling Guidelines
- Data Protection Impact Assessment (DPIA) Procedure
- CCTV Policy
- Policy for Responsible Computing
- Research Ethics Policies and Procedures
- Safeguarding Policy

4. Definitions

For the purposes of this policy:

- **Personal Data** means any information relating to an identified or identifiable natural person.

- **Data Subject** means an identified or identifiable natural person whose personal data is processed.
- **Processing** means any operation or set of operations performed on personal data.
- **Data Controller** means the natural or legal person or body which determines the purposes and means of processing personal data.
- **Data Processor** means a natural or legal person or body which processes personal data on behalf of a controller.
- **Special Categories of Personal Data** has the meaning set out in Article 9 GDPR.
- **Data Protection Officer (DPO)** means the officer appointed by MIC in accordance with Articles 37–39 GDPR.

5. Principles

MIC processes personal data in accordance with the principles set out in Article 5 GDPR:

1. **Lawfulness, fairness and transparency –** personal data is processed lawfully and transparently.
2. **Purpose limitation –** personal data is collected for specified, explicit and legitimate purposes.
3. **Data minimisation –** processing is limited to what is necessary for the stated purpose.
4. **Accuracy –** reasonable steps are taken to ensure personal data is accurate and up to date.
5. **Storage limitation –** personal data is retained only for as long as necessary, in accordance with MIC's Records Retention Schedule.
6. **Integrity and confidentiality –** appropriate technical and organisational measures are applied to protect personal data.
7. **Accountability –** MIC is responsible for, and able to demonstrate, compliance with these principles.

6. Data Subject Rights and Erasure

MIC recognises and supports the exercise of data subject rights provided for under the GDPR, including the rights of access, rectification, restriction, objection, data portability and erasure.

The right to erasure pursuant to Article 17 GDPR is not absolute. MIC may lawfully refuse a request for erasure where the continuing processing of personal data is necessary for:

- Compliance with a legal obligation;
- The performance of a task carried out in the public interest or in the exercise of official authority;
- Archiving purposes in the public interest;
- The establishment, exercise or defence of legal claims; or
- Compliance with statutory or regulatory retention requirements.

Where a request for erasure is refused, MIC will provide the data subject with the reasons for the decision and information on their right to lodge a complaint with the Data Protection Commission.

7. Responsibilities

Governing Body

The Governing Body has overall responsibility for ensuring that appropriate governance, oversight and accountability arrangements are in place to support MIC's compliance with Data Protection Legislation.

Executive Management / Senior Management

Senior management is responsible for ensuring that this policy is implemented effectively across the College and that adequate resources are made available to support data protection compliance.

Information Compliance Office and Data Protection Officer (DPO)

The Data Protection Officer provides independent advice and guidance on compliance with Data Protection Legislation, monitors compliance with this policy and related procedures, and acts as MIC's contact point with the Data Protection Commission.

Staff, Students and Third Parties

All staff, students and third parties are responsible for complying with this policy and with applicable data protection procedures when processing personal data on behalf of MIC.

8. Departure from the Advice of the Data Protection Commission

Where guidance, advice, recommendations or decisions are issued by the Data Protection Commission (DPC) in relation to MIC's processing of personal data, Mary Immaculate College is committed to having due regard to such guidance in the performance of its functions as a Data Controller.

Where MIC proposes to depart from, or adopt a position that differs from, advice or guidance issued by the Data Protection Commission:

- The relevant advice or guidance must be clearly identified and documented;
- The rationale for departing from the advice or guidance must be formally recorded;
- Any associated legal, regulatory or data protection risks must be assessed and documented;
- Accountability for the decision must rest with senior management and, where appropriate, the Governing Body;
- The decision must be taken in a manner that demonstrates respect for the role of the Data Protection Commission as Ireland's supervisory authority.

Such a decision does not diminish MIC's obligations under Data Protection Legislation and does not preclude engagement with, or review by, the Data Protection Commission.

9. Data Protection Risk Management Measures

Mary Immaculate College adopts a proactive and risk-based approach to the protection of personal data. In accordance with Article 24 and Article 32 GDPR, MIC implements appropriate technical and organisational measures to manage data protection risks and to ensure the ongoing confidentiality, integrity and availability of personal data.

MIC's data protection risk management framework includes, but is not limited to, the following key measures:

Data Protection Impact Assessments (DPIAs)

MIC undertakes Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals, in accordance with Article 35 GDPR. DPIAs are used to identify, assess and mitigate data protection risks at an early stage and to support data protection by design and by default.

The requirement for a DPIA, and the outcomes of any assessment, are documented in accordance with MIC's DPIA Procedure.

Data Security

MIC applies appropriate technical and organisational security measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage. Such measures are proportionate to the risks presented by the processing and the nature of the personal data involved.

Data security requirements are supported by MIC's Information Security policies, Personal Data Handling Guidelines and contractual obligations applied to third-party data processors.

Personal Data Breach Management

MIC has established procedures for the timely identification, assessment, containment and reporting of personal data breaches in accordance with Articles 33 and 34 GDPR. All actual or suspected personal data breaches must be reported without delay to the Information Compliance Office.

Personal data breaches are assessed on a case-by-case basis to determine notification obligations to the Data Protection Commission and, where required, communication with affected data subjects. Breach management activities are documented in accordance with MIC's Personal Data Breach Protocol.

10. Further Information

The College Privacy Notices are available to view on the MIC website Information Compliance Office | Mary Immaculate College. Further information on data protection matters for staff and students is available via the College Staff Portal and Student Portal, or by contacting dataprotection@mil.ul.ie

11. Policy Review

This policy will be reviewed every three years or sooner if significant legislative or technological changes occur.

12. Revision History

Revision	Document History	Reviewed By ET	Approved By UR
0	Initial Release	---	BR2013#02
1	Amendment	ET2018#09	UR2019#01
2	GDPR aligned policy rewrite. Inclusion of erasure policy and governance where DPC advice is not followed.	ET2026#05	UR2026#03