BRIATHAR DÉ MO LÓCHRANN

MIC

MARY IMMACULATE COLLEGE
COLÁISTE MHUIRE GAN SMÁL

Records Management

1. Policy Statement

Mary Immaculate College (MIC) acknowledges that the effective management of its data and records is essential to support its core operations, ensure compliance with legal, statutory, and regulatory obligations, protect personal information, and facilitate the efficient management of the organisation.

This policy, along with associated documentation, adheres to the standards and expectations set by contractual and legal requirements and is designed to align with best practices in records management. The goal is to implement a structured approach to document control. This policy applies equally to records created and preserved in electronic and paper formats.

Proper and efficient management of data and records is essential to:

- Ensure that the College operates in a structured, efficient, and accountable manner.
- Maximise value through improved information quality, better coordination of records, and enhanced storage systems.
- Support core business functions by providing evidence of proper conduct and the maintenance of systems, tools, resources, and processes.
- Comply with legislative, statutory, and regulatory requirements.
- Deliver consistent and fair services to staff members, students, clients, and stakeholders, and protect their interests.
- Assist in the development of policies and managerial decision-making.
- Provide continuity in the event of a disaster or security incident.
- Safeguard personal information and uphold data subject rights.
- Prevent the use of inaccurate or misleading data and minimise risks to personal information.
- Ensure data is erased in accordance with legislative and regulatory requirements.

Retaining information longer than necessary introduces additional risks and costs and may violate data protection principles and laws. MIC retains records and information only for legitimate or legal business purposes and fully complies with data protection laws, regulations, and best practices at all times.

2. Purpose

The purpose of this Records Management Policy is to establish a framework for the effective management of College records, ensuring compliance with legal obligations, operational efficiency, and historical preservation.

3. Objectives

The objectives of this policy are to:

- Provide guidelines for the creation, classification, retention, and disposal of records.
- Support operational efficiency by ensuring timely access to relevant information.
- Safeguard sensitive and confidential data from unauthorised access or loss.
- Ensure compliance with industry regulations, legal obligations, and governance standards.
- Mitigate risks related to audits, legal disputes, and data breaches.

- Preserve historical and essential records that support organisational accountability and continuity.

By implementing this policy, MIC strengthens transparency, responsibility, and efficiency in records management.

4. Scope

This policy applies to all staff (full and part time), agency staff, external contractors, and researchers who handle College records in any format (physical or digital) as part of their employment duties. Each has a responsibility to ensure that they handle records in accordance with the conditions set down in this policy, the MIC Records Retention Schedule and any other relevant College policies, regulations, and procedures.

This policy is relevant to all departments, faculties, administrative units, research centres, and areas of work which form part of the College structure. For the purposes of this Policy, references to the above will be shortened to "Functional Area."

This policy applies to all records of the College.

5. Related Documents

5.1 Legislation

Code	Legislative Title	Revision
	General Data Protection Regulation (GDPR) (EU) 2016/679	
	Data Protection Act 2018	
	Freedom of Information Act 2014	
	National Archives Act 1986	
	Education Act 1998	
	Universities Act 1997	

5.2 MIC Policies

Code	Policy Title	Revision
PGP-036	Data Protection Policy	02

5.3 MIC Procedures and Forms

Code	Process Title	Revision
	MIC Records Retention Schedule	
	Data Breach Notification Form	
ICP-006	Procedure for Offsite Storage and Blank Storage Grid	00
ICP-047	Accessing Archives Request	00
ICP-050	Guidelines for Completing a RoPA and Blank RoPA Template	00

6. Definitions

6.1 Record

A record means any information created or received, and maintained by the College in the course of its official business.

6.2 Records Management

The systematic control of records throughout their lifecycle: creation, use, storage, and destruction or archiving.

6.3 Personal Data

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;

6.4 Records Retention Schedule

A Records Retention Schedule is a control document that describes the College’s corporate records at a series level, and:

- specifies the length of time each record should be retained prior to final disposition;
- specifies the final disposition route of each record;
- serves as the legal authorisation for the disposition of records.

6.5 Disposition

Disposition means the action taken in regard to the disposal of active records, which can involve physical destruction by means of security shredding or recycling; transfer to archival storage for selective or full retention; or special disposition though a formal act of alienation from the custody of the College.

6.6 System

A system means a hardware unit, software program and/or business process used by staff to help achieve a given business purpose (e.g., student records system, employee records system, etc). It is the responsibility of the System Owner (the Head of the functional area that utilises the system or their nominee) to monitor and ensure compliance with this Policy by employees involved in the use of the system.

6.7 Staff

Staff means all full-time and part-time employees of the College, staff funded externally but under contract to the College, including seconded staff, placement students employed by MIC and researchers under contract to the College.

6.8 Students

Student means all full-time and part-time registered students at the College.

6.9 RoPA

RoPA means a Record of Processing Activities[1]. Each office/department/unit within the College must have an area specific RoPA. Directors/Heads of Department are responsible for the maintenance of each their respective RoPAs. ICO is responsible for managing the co-ordination and update of the overall College RoPA based on the area specific RoPAs submitted to ICO. RoPAs are reviewed by ICO on an annual basis.

6.10 Data Processing Activity

A data processing activity refers to any operation or set of operations performed on personal data. It can include collecting, storing, organising, retrieving, sharing, or disclosing, deleting, or erasing data.

7. Principles

The General Data Protection Regulation (GDPR) establishes seven core principles that underpin responsible records management and data handling. These include:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality; and
7. Accountability

These principles guide how personal data should be collected, stored, used, and disposed of, ensuring that records are managed in a way that respects individuals' rights and complies with legal obligations. Adherence to these principles is essential for maintaining trust, safeguarding privacy, and supporting the lawful operation of all institutional activities.

8. Responsibilities

8.1 Staff

All staff are responsible and accountable for creating and keeping accurate and complete records of their business activities. This includes records and data created in the course of carrying out or contributing to research (see Data Protection Research portal page). Staff must ensure that the records and data for which they are responsible are securely managed in a manner which is compliant with this policy, related College policies, and relevant procedures, including the MIC Data Protection Policy, IT Security Policy, and future Data Classification Procedures.

8.2 Data Champions

Data champions may be appointed by Heads of Department or Heads of Faculty to take day-to-day responsibility for records management processes (e.g., security, transfer, disposal), to support other staff in performing such processes, to report to management, and to liaise with the Information

[1] Article 30 of the General Data Protection Regulation (GDPR) places an obligation on data controllers, such as MIC, to have in place a detailed record which accurately identifies the activities the College carries out which use **personal data**. Failure to identify all relevant processing activities may result in personal data being processed in a way that is not in compliance with the GDPR

Compliance Office. The identity of data champions should be recorded and known to all staff in the relevant unit. The general functions of a data champion are set out in a guideline on the ICO Portal Page.

8.3 Data Owners

Data Owners are generally the most senior person in a functional area. In the case of MIC, operational responsibility for records rests with each Director or Head of Department and each Head of Faculty in Faculty offices.

Data owners have overall and operational responsibility for records management implementation and compliance within their functional area or area of work. This includes the following:

- authorising access to and processing of records and data and assigning responsibilities;
- ensuring adequate training and guidance is given and facilitated;
- managing risk and ensuring appropriate security and destruction arrangements are in place;
- approving actions as required under records management procedures and RRS;
- ensuring standard and local procedures, e.g., for digital systems used in their area, are applied, and developed where necessary;
- ensuring processing activities carried out on their behalf comply with this policy and other relevant College policies, all applicable legal requirements, and any applicable contract or agreement.

The Data Owner retains overall responsibility for the records or data concerned. Where a Data Controller (MIC) engages a Data Processor (external service provider) to carry out processing on its behalf, there is a statutory requirement that a contract in writing must be entered into between the parties, governing those processing activities.

Where students and other users process and/or gain access to records and data created in the course of College activities, they are subject to the requirements of this policy relating to all processing activities.

9. Classification of Records for the Records Retention Schedule

In accordance with this Records Management Policy, records within the College are classified based on their function, significance, and applicable retention requirements. This classification ensures proper storage, retrieval, and disposal of records in compliance with legal, regulatory, and operational needs.

9.1 Record Categories

Records are classified into the following broad categories:

- **Academic Records** (student applications, transcripts, examination results, syllabi, placement reports)
- **Administrative Records** (strategic plans, committee minutes, institutional reports)
- **Financial Records** (invoices, payroll records, budgetary documents, audit reports)

- **Human Resources Records** (staff contracts of employment, training records, pension records, leave records)
- **Research Records** (funding applications, ethics approvals, research publications, project data)
- **Legal & Compliance Records** (contracts, data protection agreements, institutional policies, FOI records, legal advice, confidentiality agreements)
- **Facilities & Infrastructure Records** (property deeds, maintenance logs, equipment inventories, CCTV footage)

9.2. Retention Periods & Disposal Actions

Each record category is assigned a retention period based on College policies and statutory requirements. Once the retention period has expired, records may be:

- **Archived** for historical or compliance purposes
- **Securely destroyed** if no longer needed
- **Transferred** to designated external bodies when applicable

9.3. Compliance & Oversight

Records classification and retention must adhere to the National Archives Act 1986**,** GDPR regulations, and relevant guidelines from regulatory bodies such as the Higher Education Authority (HEA)**.** College staff are responsible for maintaining and enforcing proper records management practices.

This structured approach to classification ensures that records are managed consistently and responsibly, supporting the College's operational efficiency and legal compliance.

10. Management of College Records

All records created by staff in the course of their duties on behalf of the College are retained for as long as required to meet the legal, administrative, financial, and operational requirements of the College, after which time they must be either destroyed or transferred to the College Archives. The final disposition (either destruction or transfer to the Archives) of records is carried out according to approved schedules as outlined in the MIC Records Retention Schedule.

While the records schedules prescribe the minimum period that College records must be retained, offices may, at their discretion, keep the records for a longer period of time if it is deemed necessary.

11.Record Retention Procedures

11.1 The department/office/unit creating a new record must determine the retention period for that record as well as the final disposition of that record (i.e., confidential shredding/secure electronic deletion, archive, or transfer to designated bodies, where applicable). A record may fall into a category already listed on the MIC Records Retention Schedule (RRS). If relevant, the record should be included in the office RoPA.

11.2 Where a new data processing activity has been created, the data champion or data owner must notify the Information Compliance Office of this new activity, the retention period of the associated records and the final disposition for the records by emailing dataprotection@mic.ul.ie

11.3 ICO will review the information and consider whether to:

a) update the RRS, as appropriate, and/or
b) update the relevant area specific Record of Processing Activities (RoPA) where the record is not relevant for publication on the RRS (i.e., too granular)

11.4 After the records have been retained by the creating offices (in situ or off-site storage) for the requisite time as stipulated in the RRS, they are either destroyed (by confidential shredding or electronic deletion) or stored in the local College Archive or other approved storage, for permanent retention.

11.5 The College’s Record of Processing Activities (RoPA) identifies the activities the College carries out which use **personal data** and the corresponding legal basis and retention period for each activity. It requires input from each area of responsibility within the College and is updated on an annual basis. The RoPA is broader and more granular than the RRS and contains the retention period for each processing activity identified therein. The College RoPA feeds into the RRS, where applicable. The RRS is broader than the RoPA as it includes corporate data that may not have personal data included.

11.6 Please refer to ICP-006, ICP-047 and ICP-050 for further information on procedures on archive requests, storage requests and completing a RoPA. For information on confidential shredding, contact buildingservices@mic.ul.ie

12. Digital Records and IT Systems

All electronic records must be stored in approved systems that support searchability, metadata tagging, version control, and secure access. For further information please contact the ICTHelpdesk.

13. Policy Review

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

14. Revision History

Revision	Document History	Reviewed By ET	Approved By UR
0	Initial Release	ET2026#04	UR2026#03