BRIATHAR DÉ MO LÓCHRANN

MIC

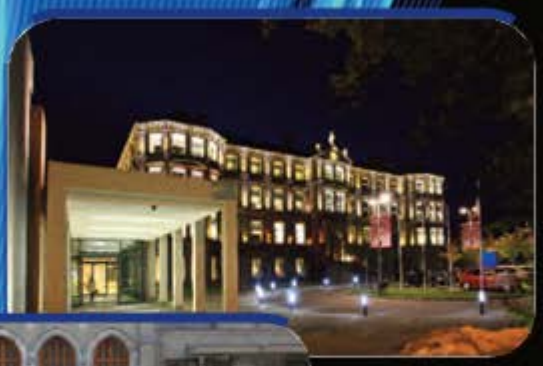
MARY IMMACULATE COLLEGE
COLÁISTE MHUIRE GAN SMÁL

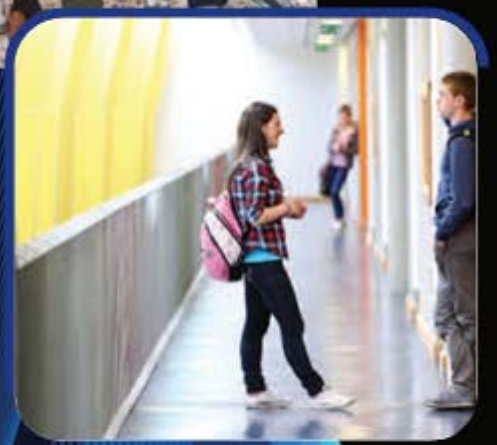
Quality Review

Peer Review Report

Information Compliance and Records Management Office

February 2022





Contents

1. Introduction

1.1 Quality at MIC

MIC's quality review process, as applied to both academic departments and professional services, was developed and continues to evolve in order to satisfy college quality policy and meet legislative QA requirements.

MIC complies with the Qualifications and Quality Assurance (Education and Training) Act 2012, which places a legal responsibility on the provider and linked provider to establish procedures in writing for quality assurance for the purposes of establishing, ascertaining, maintaining and improving the quality of education, training, research and related services. (Part 3, Section 28).

These QA procedures must take due account of relevant quality guidelines issued by Quality and Qualifications Ireland (QQI) and/or predecessor organisations. QQI is the statutory body responsible for reviewing and monitoring the effectiveness of QA procedures adopted and implemented by higher and further educational institutions within Ireland.

The periodic quality review of functional areas (academic and professional service) within the College represents a cornerstone institutional QA/QI mechanism.

MIC's Quality Review Process

The purpose of the quality review process is:

- To provide a structured opportunity for the professional service to engage in periodic and strategic evidence-based self-reflection and assessment in the context of the quality of its activities and processes, and to identify opportunities for quality improvement
- To provide a framework by which external peers, in an evidence-based manner, can independently review, evaluate, report upon and suggest improvements to the quality of the professional service's activities and processes
- To provide a framework by which the professional service implements quality improvements in a verifiable manner
- To provide MIC, its students, its prospective students and other stakeholders with independent evidence of the quality of the professional service's activities
- To ensure that all MIC professional services are evaluated in a systematic and standardised manner in accordance with good international practice and in support of the objectives of the College's Quality Policy
- To satisfy good international practice in the context of quality assurance in higher education and to meet statutory QA requirements as enshrined in national law

1.2 Overview of the Quality Review Process for Professional Services

The quality review process for MIC Professional Services consists of three phases:

- Self-Assessment
- Peer Review
- Quality Improvement

Self-Assessment

Self-assessment is the first phase of the quality review process and takes approximately 6 months. It culminates in an analytical, evidence-based, Self-Assessment Report (SAR), which is written by the relevant professional service.

Peer Review

In the Peer Review phase, the members of the Peer Review Group (PRG) read the Self-Assessment Report and either spend a number of days in the college or conduct the review remotely. The review group completes a Peer Review Report (PRR) on its findings that comprises both commendations and recommendations.

Quality Improvement

The Quality Improvement phase comprises the following stages:

- Consideration of recommendations by the professional service and formulation of a Quality Improvement Plan (QIP);
- Identification of SMART (specific, measurable, achievable, realistic and timed) action items necessary to implement the recommendations;
- Ongoing implementation of recommendations;
- Interim progress report to Quality Committee.

1.3 Information Compliance and Records Management (ICRM) Office

As a publicly-funded body, Mary Immaculate College is subject to Irish Freedom of Information legislation. Like all organisations controlling data that includes personal information (e.g. students, staff, applicants for courses or applicants for employment), the College also abides by Irish Data Protection legislation and it operates within the General Data Protection Regulation (GDPR) framework.

The meeting of these requirements together with related continuous quality improvement processes is managed by the Information Compliance and Records Management Office. Other work undertaken by this office includes records management as well as risk management in respect of the data control environment, together with provision of advice and guidance to units of the College that require support for the generation of contracts or Memoranda of Understanding (MoUs) where exchange of personal or commercially sensitive information occurs.

1.4 Peer Review Group Observations

Aileen O'Sullivan, Data Protection Officer at Limerick & Clare Education and Training Board and Eileen Jackson, Data Protection Officer at Marino Institute of Education comprised the Peer Review Group (PRG) along with Garrett Greene, Data, Governance & Compliance Officer at Technological University of the Shannon, who chaired the PRG.

This report is the final output from processes undertaken over a period between November of 2021 and February 2022.

In December of 2021, the Peer Review Group considered the Self-Assessment Report of the Information Compliance and Records Management Office (ICRM) at Mary Immaculate College (MIC) - which had been prepared the previous month - and the 20 'Planned Improvements' that it identified, as well its 6 further substantive recommendations.

The PRG submitted a Pre-Visit Summary of Initial Findings on 5th January 2022 and conducted its site visit between 12th and 14th January 2022. It presented an initial draft of its final report on the final day of that visit and it is submitting this report in February 2022.

The PRG wishes, at the outset of this report, to recognise and commend the dedication and professionalism of the staff of the ICRM Office, led by Elaine Mulqueen, and to acknowledge their considerable work, knowledge and achievement in delivering a very high quality of service to MIC.

The PRG recognises that the review process has placed an additional workload on each member of staff of the ICRM Office and wishes to commend their openness and willingness to engage in this worthwhile exercise.

The PRG wishes to record its very deepest gratitude to Quality Assurance Manager Emma Barry, whose kind assistance and patient facilitation were unflinching from outset to conclusion. Emma's responsiveness and professionalism were of immense value to the PRG as it worked through the process.

Meetings undertaken provided further insights into the ICRM function of the College and informed the PRG's commendations and recommendations. The PRG wishes to record sincere gratitude to all colleagues at MIC who so readily and freely made available their time, their knowledge and the additional information requested by the PRG.

In the order in which we met them in the course of our visit, these particularly include Vice President of Governance & Strategy Professor Gary O'Brien, Director of Quality Dr Deirdre Ryan, Information Compliance Manager Elaine Mulqueen, Director of ICT Services Kieran Pearse, Project Portfolio Manager ICT Martin Waters, Data Champions Shirley Kearney, Rob O'Halloran and Dr Fiona McDonagh and Vice-President of Administration & Finance Michael Keane.

The scope of the quality review as determined by the MIC Quality Committee was for the Peer Report Group to:

- Independently review, evaluate, report upon and suggest improvements to the quality of the professional service's activities and processes.
- To provide a framework by which the professional service implements quality improvements in a verifiable manner.
- To provide MIC, its students, its prospective students, its staff and other stakeholders with independent evidence of the quality of the professional service's activities.
- To ensure that all MIC professional services are evaluated in a systematic and standardised manner in accordance with good international practice and in support of the objectives of the College's Quality Policy.
- To satisfy good international practice in the context of quality assurance in higher education and to meet statutory QA requirements as enshrined in national law.

The PRG, enabled by the willing and open assistance of MIC contributors, has concluded upon its own independent evaluation.

This PRG believes the recommendations made and the planned improvements endorsed are clear and specific, lending themselves to verifiable implementation.

The PRG engaged in rigorous enquiry, particularly during our visit and engagement with MIC colleagues, that should provide stakeholders with confidence in our independent assurance that a high standard of Data Protection and Information Management practice is in place at MIC.

The PRG has followed the Quality Review process in all of the detail and rigour set-down by MIC to meet the statutory requirement for a quality assurance procedure aligned to good international practice.

2. Structure, Governance and Mission

2.1 Commendations

2.1.1	The clear individual professional capabilities and personal commitment of the ICRM Team provides a fundamental level of assurance of dedication to good practice in Data Compliance and Information Management.
2.1.2	That the Office can draw clear link between its practice and the current and former strategic plans of MIC indicate its commitment, as a corporate entity, to good practice in Data Compliance and Information Management.
2.1.3	The fact that MIC has procured a dedicated system (Privacy-Engine) as an enabling tool for the monitoring and control of Data Compliance and Information Management indicates a willingness not just to commit but to invest.

2.2 Recommendations

	Recommendation	Rationale
2.2.1	The PRG endorses the recommendation at point 2.4.5 of the SAR, that the DPO function should be repositioned at a level between ICM and the VPGS	Articles 37-39 of GDPR make it a legal requirement that the DPO be organisationally positioned at a high level of authority and that the role be appointed such that any other functions or duties it may carry must not conflict with its duty to ensure that rights and obligations under the GDPR are vindicated. The PRG is aware that conversations in other areas of the Higher Education sector had, for instance, considered placing DPO duties at a management level below that of the Executive and tying-in other compliance, risk, governance duties that complement rather than conflict with the DPO duty. Such an appointment, even carrying other governance/compliance duties, would enhance the resources at the disposal of ICRM and ensure greater support to the ICM.
2.2.2	The PRG endorses that element of the recommendation in the SAR at 2.4.5 that calls for a realistic assessment of the necessary resources to maintain day-to-day operations within ICRM.	The PRG is concerned that the degree to which Data Compliance responsibilities, duties, functions – operationally and strategically – rest on the ICM individually is not sustainable and poses a business continuity and compliance risk to MIC. Fulfilment of the immediately previous recommendation would also part in the

		assuring appropriate enhanced resourcing of ICRM.
2.2.3	Furthermore, the PRG takes the view, based on its own user-experience, that the deployment of Privacy-Engine with its full functionality may have potential to save considerably on the human resource input necessary to enable effective ongoing monitoring and control of compliance. This deployment, in itself, however, will require some resourcing for an implementation period. This should urgently be considered.	In an Employment Control Framework context and a context of competing demands for human resource, it is essential that systems that have the potential to drive process efficiency be fully utilised. Temporary application of Human Resources to an implementation, to ensure none of its potential goes untapped, can play a role in the medium to longer term saving on Human Resource.
2.2.4	There is scope for an operational as well as a messenger/advocate role for the Data Champions Network. One example of this might be for the Data Champions to become active Privacy-Engine users, updating the Registers of Processing Activity for their own individual areas. The recommendation is that a working review be conducted with a view to reframing and stating the role of the Data Champion in measurable, operational and deliverable terms in addition to its important advocacy work, (which should continue).	The network appears to be enthusiastic and engaged for the most part. This creates potential for sections, departments, offices, services to whom responsibility for Data Compliance is distributed to actively contribute to its management in a way that bears some of the weight that currently rests on ICRM.

3. Information Compliance & Records Management Office Functions

The key functions of the ICRM Office are:

1. Policy Development
2. Quality Assurance & Enhancement
3. Records Management
4. Statutory Compliance
5. Risk Management & Internal Control
6. Training & Awareness
7. Advice & Guidance

3.1: Policy Development

3.1.1 Commendations

3.1.1.1	Well-structured policy drafting framework with all relevant stakeholders consulted
3.1.1.2	The seeking of stakeholder feedback on Information Compliance and Data Protection awareness is a positive and information action
3.1.1.2	Recognition of the constraints within the procurement framework for advice but making use, nonetheless, of Privacy Engine advisory support.

3.1.2 Recommendations

	Recommendation	Rationale
3.1.2.1	Explore the use of Privacy Engine for dissemination of policies to staff and for highlighting when policies are due for review.	Under the current mechanisms the onus on the staff member to read relevant policies cannot be monitored and it would appear to be beneficial automate the flag that a policy is due to expire.
3.1.2.2	The PRG recommends that ICRM consider initiating the development of a Peer Network at a local/regional level among public bodies with similar challenges.	The former 'Shannon Consortium' colleges and the local Further Education Sector will offer support on an ad-hoc and non-structured basis currently and some formalisation of those existing relationships may be the optimal solution. Drawbacks to the formal operation of the larger networks of Information Compliance Officers have been highlighted in the form, for example, of unevenly distributed contribution to working groups etc.

3.2: Quality Assurance & Enhancement

3.2.1 Commendations

3.2.1.1	The awareness levels reported from survey feedback are reassuring and provide measured evidence of the penetration of good Data Compliance and Information Management practice.
3.2.1.2	The QMS document is comprehensive in respect of the office functions, procedures and how to access those etc. A clear, comprehensive 'playbook' of this type is a key initial part of ensuring good practices can be followed and implemented around the organisation.

3.2.2 Recommendations

	Recommendation	Rationale
3.2.2.1	Please see recommendations at 3.5 that have implications for Quality Assurance & Enhancement.	See 3.5

3.3: Records Management

3.3.1 Commendations

3.3.1.1	A system in place for issuing reminders to staff of records whose retention periods are about to expire is a very worthy systems and should be retained. This is further measured evidence of good practice in situ.

3.3.2 Recommendations

	Recommendation	Rationale
3.3.2.1	Please see recommendations at 3.5 that have implications for Quality Assurance & Enhancement. The Recommendation within the SAR, at 3.3.7 states *"As a function of due diligence and as expressed by a relevant protocol and internal control, the ICRM Office should be involved in projects that involve the generation of records from the outset…"* This is a worthy recommendation and the PRG's recommendation at 3.5 may help to operationalise the line-of-sight required to know what record-generating projects are taking place around MIC. The 'protocol' and 'internal control' might be identified from the substantive recommendation at 3.5	A standing suite of items to be addressed within a rolling review process can encompass this recommendation – see point 3.5 The PRG not alone endorses the recommendation of the SAR at 3.3.7 but it considers it essential that it also identify what protocol or internal control can operationalise the principle involved. Operationalising this principle is more than good practice. The requirement to demonstrate 'Data Protection by Design' in the implementation of new processes and technologies is a legal requirement under GDPR Article 25.

3.3.2.2	The PRG endorses the planned improvements specified at 3.3.6 and recommends that these should be proceeded with.	As above

3.4: Statutory Compliance

3.4.1 Commendations

3.4.1.1	The College has a formalised and well-structured "critical path" for the management of requests under FOI and Data Protection SAR regimes in evidence of good practice.
3.4.1.2	Guidance for staff is available the in "Guidelines for Staff on Receipt of an FOI" request.
3.4.1.3	Use of templates and forms for co-ordinating requests should help to ensure clarity and consistency.
3.4.1.4	Appropriate Subject Access Rights Request Procedures are in place.
3.4.1.5	It is essential to building a compliance culture that the ICRM office continuously works towards removing the "Fear Factor" when reporting breaches. That it does this, that it does not assign blame and that it operates in a spirit of collaboration around these duties is highly commendable practice.
3.4.1.6	Constant awareness-raising and controls in place regarding the need for Data Processing Agreements between the College and external parties are commendable actions / processes that evince good practice in situ.
3.4.1.7	The PRG is impressed by the range of communication streams that the ICRM uses and finds the variation of communication practices to be very highly commendable – bulletins, emails, newsletter, coffee mornings, champions networks etc.

3.4.2 Recommendations

	Recommendation	Rationale
3.4.2.1	The PRG recommends in the context of fully-operationalising Privacy-Engine, that the following processes be adopted: • SAR and FOI should be recorded in Privacy Engine. • Integration of risks identified by PrivacyEngine into the ICRM Risk Register. • Assignment of risks on Privacy Engine to appropriate owners within MIC who will then be responsible for the mitigation actions.	This recommendation will make for a more efficient use of time, it will hold all correspondence in a single repository, it will make SAR, FOI and Data Risks amenable to the Privacy Engine reporting features and will distribute the responsibility for Data Compliance throughout the organisation in line with policy.

3.5: Risk Management & Internal Control

3.5.1 Commendations

3.5.1.1	The initiative of creating Annual Service Plans is welcome
3.5.1.2	The desire to create internal control frameworks for annual testing by ICRM is welcome

3.5.2 Recommendations

	Recommendation	Rationale
3.5.2.1	The PRG recommends that a process of rolling-review, incorporating a review of ROPA, current physical and electronic storage practices, external relations and DSAs, new processes and technologies and compliance with retention schedule should be put in place and it should engage each office, faculty, service of MIC and be incorporated within the Annual Service Plan of ICRM.	This practice will enable the regular check on records retention, DSAs and the appropriateness of processing – as well as updating ROPA – that are elsewhere referenced in the SAR. It will also ensure that ICRM is aware of any new processes that may not have had to go through procurement or ICT implementation that involve either the generation of new records or new personal data processing, (and that might thus require DPIA). Furthermore, these reviews may become problem-solving workshops for individual offices and services and they will broaden the visibility and reach of ICRM beyond the Data Champions Network. This practice had been in place at the former Limerick Institute of Technology (LIT) and remains part of Data Compliance and Information Management practice for that entity of Technological University of the Shannon (TUS) as that organisation continues on the path of integration. Experience-sharing and benchmarking in relation to this is available from TUS. Such a process will help to either satisfy or monitor, in full or in part, a number of the legal requirements of GDPR: Article 39(1)(b): Requirement to monitor and audit. Article 25: Data Protection by design and default. Article 5: Requirement to comply with the GDPR Data Processing principles: Lawfulness & Transparency; Purpose Limitation; Data Minimisation; Accuracy; Storage Limitation; Integrity and Confidentiality.

3.6: Training & Awareness

3.6.1 Commendations

3.6.1.1	The parallel operations to train all Data Champions and Staff is highly commendable and it is furthermore commendable that the mandatory element of GDPR training encompasses five discreet modules.
3.6.1.2	The availability of ICRM to meet face-to-face group and bespoke training needs is valuable and commendable.
3.6.1.3	The communications work positively referenced at point 3.4.1.7 above is of key relevance here also.

3.6.2 Recommendations

	Recommendation	Rationale
3.6.2.1	The PRG recommends that ICRM liaise with key stakeholders, (e.g. ICT), to examine the potential for Privacy-Engine to provide a single, traceable platform for training delivery and participation, (mandatory and optional), across the elements of the organisation that target training at various staff and/or student cohorts.	The key stakeholders with an interest in ensuring that staff have knowledge of relevant policies and good practices will all benefit from having a single tool for delivery and tracking participation in training.
3.6.2.2	The PRG recommends that the highest levels of governance and leadership at MIC should communicate to all management and staff that mandatory training is designed to protect the rights of staff and students and must be undertaken fully and without exception.	Mandatory training is designed to enhance no more than the protection and vindication the rights and interests of all staff, students and the community of MIC.
3.6.2.3	The PRG endorses the planned improvements and recommends they should proceed (SAR Section 3.6.6).	The planned improvements in this area particularly demonstrate a spirit of ongoing self-evaluation, innovation and continuous improvement.

3.7: Advice & Guidance

3.7.1 Commendations

3.7.1.1	The flexibility and responsiveness of ICRM is clear in the context of COVID, for example, and is borne-out for mention elsewhere in this document in relation to statutory compliance and training and awareness in particular.

3.7.2 Recommendations

	Recommendation	Rationale

4. Environment and Facilities

4.1 Commendations

4.1.1	The location of the VPGS's office side-by-side with ICRM is important in a complex and growing organisation where adjacency can be an aid to visibility and priority.
4.1.2	The use of individual access codes for printers is an important aid to protection of personal data.
4.1.3	Facilities provided to staff, as described in the SAR, appear to be excellent.
4.1.4	Seamless adaptation to the multi-campus environment and provision of multi-campus service is highly commendable.

5. Organisation and Management

5.1 Commendations

5.1.1	In the ever-evolving world of cyber risk, ICT systems protections can never be said to be fool-proof, impenetrable, beyond the reach of nefarious activity. The PRG is hugely reassured by the suite of layered security controls in place in terms of these amounting-to, in many cases, as much as it is reasonably practicable and possible to do to ensure appropriate protection of systems from unauthorised or nefarious external access and appropriate control of access internally for users within the system. These include: • Careful asset Management – move from desktop to laptop – tracking of what devices are deployed and where. • Software management • Perimeter Control: Firewall, Fortinet. • Network: Segregated Network: Staff VLAN, Student VLAN, Visitor VLAN. • Device: Endpoint security – Kaspersky, Server – Webroute, Mobile – Mobile Iron. • Application accesses integrated to active directory and Office365. • Multifactor Authentication to access the VPN remotely. • Multifactor Authentication for as many individual systems as possible. • Patch management – regular test and patch of non-Microsoft elements. • Aiming for the ISO standards through the Deloitte controls framework, (all aligned to ISO 27701) • Data Centres have physical card access and alarmed locations. • Managing on key principles of Confidentiality, Integrity, Availability • Advisory flag on all emails from external sources. • Control protocols for use of freeware or applications that don't have to go through procurement and no purchase of software without central ICT control: compliance with procurement, security and data-compliance rules and DPIA, • Moodle management: Office365 account as a first prerequisite for access; (*leavers* and *leaves-of-absence* are made dormant or extinguished; starters and leavers policy). Moodle upgraded annually each Summer. Previous years Moodle archived. Held to specified date in the calendar to accommodate, appeals, resits,

	repeats, exam-boards etc and then deleted. Automation underway to ensure that only students associated with a particular key can access the Moodle but that they can do so automatically Control of external users being exclusive to ICT. • Regular Phishing, Malware, Ransom-Ware training and awareness programmes.

5.2 Recommendations

	Recommendation	Rationale

5.2.1	The PRG recommends that actions to raise the profile and visibility of ICRM should include the positioning of either ICM or a newly repositioned DPO at a number of points in committees and boards structures of the College:
	
	- ICT Committee
	- Standing Report to ARC
	- Attendance at Research Ethics Committee
	- Mandated (by Academic Council in the context of appropriate internal control) periodic attendance at:
	  ○ Faculty Management Committee
	  ○ Faculty Board
	
	It is recommended too, that Academic Council make a determination as to what other academic fora Data Compliance ought to appear at in order to assure internal control. This must include the governance structures of the Research and Graduate School.
		The legal requirement for Data Protection by design and default under GDPR Article 25 cannot be satisfied in a large, complex and personal-data-intensive organisation unless the frontline Data Compliance practitioners enjoy appropriate:
		
		• ***Lines of sight*** of activity taking place around the organisation
		• ***Lines of visibility*** to the key decision makers and implementers as they take actions that impact upon personal data processing
		
		The key risks to Higher Education Institutes of attracting negative attention from the Data Protection Commissioner will arise from a failure to see the compliance risks as they materialise or to obtain helpful advice on the compliant path to goal at an early stage in any process.
		
		This is why it is in the interests of all actors that the Data Compliance implementers enjoy those relevant lines of sight and visibility at all times.

Annex 1: Peer Review Group Members

Mr Garrett Greene *Governance & Compliance Officer* *Technological University of the Shannon: Midlands Midwest*
Ms Aileen O'Sullivan *Compliance Officer* *Limerick and Clare Education and Training Board*
Ms Eileen Jackson *Data Protection & FOI Officer* *Marino Institute of Education*

Annex 2: Schedule of Meetings with Stakeholders

A list of the stakeholders that met with the Peer Review Group will be added once this is agreed.

- Quality Assurance Manager
- Director of Quality
- Information Compliance and Records Management Office Team
- Information Compliance Manager
- Vice President of Governance and Strategy
- Vice President of Administration and Finance
- Representatives of the Data Champions Network including Professional Services, Remote Campus and Academic staff.
- Director of ICT Services
- Project Portfolio Manager ICT Services