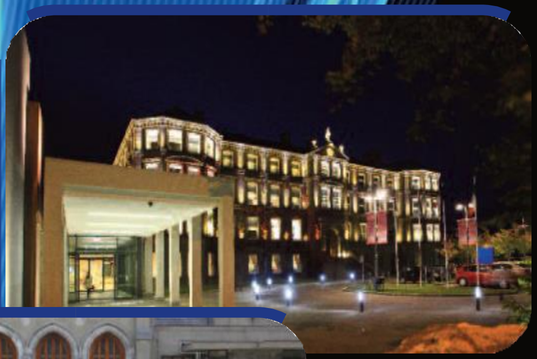
BRIATHAR DÉ MO LÓCHRANN

MIC
MARY IMMACULATE COLLEGE
COLÁISTE MHUIRE GAN SMÁL

Information Compliance Office QIP Final Progress Report

Date: 31 October 2024



Contents

Final Progress Report

This report sets out the key actions that have been undertaken to deliver on the recommendations of the Information Compliance Office Quality Review. This final progress report maps the progress of the recommendations from the drafting of the Quality Improvement Plan (QIP) in May 2022 and, presents the final status for each recommendation.

The review process consists of the following stages:

Table 1: Review Process - Stages and Timeline

Stage	Process	Timeline
1	Initiation of the Quality Review	4th March 2020 Review put on hold due to COVID
2	Development of a Self-Assessment Report (SAR)	SAR completed November 2021
3	External Assessment and **Site Visit** by the Peer Review Group	February 2022
4	Publication of a **Peer Review Report** including findings and recommendations	June 2022
5	Adoption of a **Quality Improvement Plan** by Executive Team (ET)	10 November 2022
6	Completion of **the Quality Improvement Plan**	31 October 2024

Table 2: Summary of Status of Recommendations

Total Number of Recommendations	15
Total Number of Action Items	32
Recommendations - Completed	25(78%)
Recommendations - In Progress	5 (16%)
Recommendations- Not actionable	2 (6%)

In the following sections, recommendations that have been completed are shown in green (Table 3), those that are in progress are shown in blue (Table 4), those yet to be started in orange (Table 5.)

Table 3: Recommendations Completed

Recc. No.	Allocated To:	Recommendation	Action Item	Detail of Actions Completed
2.1.1	College Management	Reposition the DPO function at a level between ICM and the Vice-President of Governance & Strategy (VPGS).	Creation of the post of Director of Information Governance & Compliance Management (DIGCM) post at Assistant Principal Officer grade & recruitment for same.	Director of Information Governance and Compliance Management appointed in September 2022. DIGCM has taken on a large number of new projects since their appointment.
2.2.2	DIGCM	Conduct a realistic assessment of the necessary resources to maintain day-to-day operations within the ICRM function.	Assess resources to maintain day-to-day operations within the Information Compliance Office function and lead a change management process.	Assessment of Resources Complete. Staffing of the ICRM has increased to three FTE staff - DIGCM, Information Compliance Manager (HEO) and Information Compliance Officer (EO).
2.2.3	Information Compliance Office	Deploy the full functionality of Privacy-Engine to utilise the potential to save considerably on the human resource input necessary to enable effective ongoing monitoring and control of compliance.	Review the functionality available within Privacy Engine in order to maximise its use.	Review of the functionality of Privacy Engine completed. ICRM maximises the use of the Data Breach Log, FOI Log, SAR log, DPIA functionality for Corporate DPIAs, DPIA log for all DPIAs (corporate and research), training courses for all staff (PE designed the 2024 annual mandatory GDPR training module which will circulate from the PE system and be logged on the system for reporting purposes) and the valuable data protection expert support function. ICRM has also shared Privacy Engine's Procurement and Audit functionality with MIC's Procurement and Audit counterparts.

2.2.4	Information Compliance Office	Conduct a working review 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.	Review the role of the Data Protection Champions (DPCs). Explore incentives to act as DPCs. Drive to recruit more Academic DPC's to strengthen the network.	Review of the role of the DPCs complete. The Information Compliance Office has recruited a total of 34 MIC DPCs and holds quarterly DPC meetings with successful attendance rates and effective engagement.
3.1.2.1	Information Compliance Office	Explore the use of Privacy Engine for dissemination of policies to staff and for highlighting when policies are due for review.	Explore use of Privacy Engine to disseminate key policies.	Implemented the use of Privacy Engine for dissemination of policies to staff and created an SOP ICP-034 for this.
3.1.2.2	Information Compliance Office	Consider initiating the development of a Peer Network at a local/regional level among public bodies with similar challenges.	Explore interest in forming peer network with other HEIs / FEIs.	Ongoing meetings arranged with TUS, UL and LCETB, Marino, FOI Network, HEA DPO Network, IRMS network.
3.3.2.2.5	Information Compliance Office	Initiate discussion between the ICRM and ICT Services aimed at an integrated system of records storage, with formal roles and control responsibilities, as well as establishing cumulative reporting frameworks;	Liaise with ICT Services to map out systems in use, where data is stored and responsibilities for these. Discussion with DICT June 23. ICT Services to share details of all systems and where data is stored.	Approved Locations for Storage of Corporate Data available on the Staff Portal https://maryimmaculatecollege.sharepoint.com/sites/staffportal/ICTS/SitePages/Storage-of-Corporate-Data.aspx
3.3.2.2.6	Information Compliance Office	Undertake, in conjunction with the Procurement Office, a review of service procurement practice, leading to new procurement protocols and commercial service agreements, as necessary;	Review current procedures with Procurement Office.	Meeting took place with Procurement. Supplier set up form has been amended to more clearly outline when staff must contact ICRM regarding new projects that involve data processing.

3.3.2.2.8	Vice-President for Research / Vice-President of Governance & Strategy	Place a renewed focus on establishing the appropriate division of responsibility for treatment and retention of research data containing personal information as produced by the MIC academic community, as well as support for the research ethics approval process where compliant data management is a requirement;	Review of current practice as part of MIREC review.	MIC Research Ethics Report published June 2023. Author: Prof. Ciara Heavin. A Research Ethics Implementation & Facilitation Team was approved by the Executive Teams in October 2023. This group began implementing the recommendations of the Heavin Report in AY23/24.
3.4.2.1	Information Compliance Office	Record Subject Access Requests and Freedom of Information Requests in PrivacyEngine.	Input previous SA and FOI requests to Privacy Engine. Use Privacy Engine for all future SA and FOI requests, update SOPs etc. to reflect this change.	All requests are now recorded on Privacy Engine. All new requests will be uploaded in line with ICP-004.
3.4.2.1.2	Information Compliance Office	Assign risks on Privacy Engine to appropriate owners within MIC who will then be responsible for the mitigation actions.	Review risks on Privacy Engine and assign to appropriate owners.	Risks identified as part of the DPIA process for corporate projects and/or student/staff research are communicated to project/research owners in addition to risk mitigating measures.

3.5.2.1	Information Compliance Office	Put in place 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 which should engage each office, faculty, service of MIC and be incorporated within the Annual Service Plan of ICRM.	Incorporating processes into the ICRM AOP.	RoPA Review completed in 2024. Process of annual rolling review incorporated into ICRM AOP.
3.6.2.1	Information Compliance Office	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.	Privacy Engine training roll out to staff.	Continuing to use PE for Mandatory GDPR training.
3.6.2.2	College Governance – Audit & Risk Committee	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.	Audit & risk committee agree that it must be mandatory, oversight of implementation by ARC through quarterly reporting;	Training is now mandatory. DIGCM is now a member of the Audit and Risk Committee and reports annually on the training statistics of staff.

3.6.2.3.1	Information Compliance Office / HR	Request assistance from HR for the delivery of in person training, in particular organising training sessions and recording participation.	Liaise with HR to organise in-person training on FOI & DP	**In Person Training:** ICRM participate in the Staff Orientation in person training, conducted twice annually in collaboration with HR. HR maintain a record of staff that have participated in staff orientation. ICRM also give face to face training to the Post Graduate Research students, MA Taught Postgraduate students and PhD DECPsy Year 2 students annually. **Online Training** HR is responsible for rolling out new starter GDPR Awareness online modules & annual mandatory GDPR training module to all staff via Privacy Engine. The annual online bespoke Data Protection Training is sent to full time staff, hourly paid staff and external student placement supervisors, ensuring comprehensive coverage across all personnel. New starters to the College are excluded from this annual training, as they receive the new starter GDPR Awareness training modules. The 2024 staff online training module was tailored to MIC staff training needs. The content was created by ICRM and the design was developed by Privacy Engine following a procurement process. A record of participation in online training modules is maintained and is reported to the Audit and Risk committee annually.
3.6.2.3.2	Information Compliance Office / HR	Request participant evaluation for in person training.	Implement when in-person training resumes.	HR request evaluation for all training.

3.6.2.3.3	Information Compliance Office	Develop more structured training programmes to be delivered over the next 4-years. As a first step document the procedure for GDPR training to include induction training for all staff with a more tailored approach to further training which will be dependent on the role and seniority of staff.	Conduct a Training Needs Analysis based on roles & responsibilities.	ICP-049 Online Annual Data Protection Training and ICP-057 GDPR Staff Awareness Online Training for New Starters created in April 2024. Identification of tailored GDPR training modules for ICT and Marketing Professionals on Privacy. This has become standard practice.
3.6.2.3.4	Information Compliance Office	Generate reports from PrivacyEngine to enable informed decision making and service planning.	Review Privacy Engine reporting functions to identify useful reports.	Relevant reports generated periodically in PrivacyEngine to enable informed decision making and service planning.
3.6.2.3.5	Information Compliance Office	Continue to develop the Data Protection Champions network, liaise with remaining Professional Services and Academic Heads of Department to establish more Data Protection Champions.	Review and conduct Gap Analysis to ensure that all areas that process personal data have a Data Champion.	Gap analysis completed. A number of new Data Protection Champions identified from new divisions. ICRM has recruited a total of 34 MIC Data Champions and holds quarterly Data Champion meetings with successful attendance rates.
3.6.2.3.6	Information Compliance Office	Try different training methods such as scenarios and role play in in person training.	Implement different training methods when in-person training resumes.	DIGCM and ICM deliver a range of in-person training sessions utilising a variety of training methods.
3.6.2.3.7	Information Compliance Office	Offer to attend academic department meetings once a year to raise awareness among academic staff.	Meet with Professional Services and Academic Departments as requested.	ICRM staff meet with Professional Services and Academic Departments when requested.

3.6.2.3.8	Information Compliance Office	Continue to provide training and support to Data Protection Champions using PrivacyEngine.	Privacy Engine training roll out to Data Champions network. Follow up with individual DCs.	Several training courses took place on PE and Cybersecurity. Following a review of the utilisation of PE, Data Champions no longer use Privacy Engine, other than for the completion of annual training. The Data Champion role is centred around advocacy and feedback to team members.
3.6.2.3.9	Information Compliance Office	Increase awareness among students regarding how the institution protects their data and how their personal data is stored and used.	Identify ways of increasing awareness among students & implement them.	GDPR training provided to MIC BA students in 2023 and 2024 as part of the College SmARTS programme. ICRM developed a student focused Data Protection page on the MIC Student Portal with useful guides, DPIA questionnaires, template Research Data Privacy Notice, etc.

5.2.1.1	College Governance	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: o Faculty Management Committee o Faculty Board	VPGS to bring proposal to ET & UR re membership of relevant committees;	DIGCM is a member of MIREC (Research Ethics Committee), ICT Services Committee and the Audit & Risk Committee.
5.2.1.2	College Governance	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.	To be considered in conjunction with 5.2.1.1.	DIGCM is a member of MIREC (Research Ethics Committee), ICT Services Committee and the Audit & Risk Committee.

Table 4: Recommendations In progress – Implementation will be monitored via ICRM AOP

	Allocated To:	Recommendation	Action Item	Detail of Actions in Progress
3.3.2.2.2	Information Compliance Office	Review the Records Retention Schedule, adding more granularity regarding what gets retained and for how long. Consult with record owners regarding retention periods, placing the onus on them to decide on the retention period for their records, Provide advice on legislative requirements for retention where applicable;	Complete full review of Records Retention Schedule, incorporate digital records into Records Retention Schedule;	Superseded by RoPA Project 2024. Record owners consulted on retention periods as part of the 2024 RoPA review (Directors and HODs were the contact points). ICRM is in consultation with all MIC offices regarding the individual office RRSs. This project will continue into 2025.
3.3.2.2.3	Information Compliance Office	Conduct a review of adherence to the records retention schedule for both paper and electronic records;	Complete as part of review of records retention schedule;	Review of adherence to RRS did not yet commence as the RoPA Project 2024 needs to be completed first. We plan to initiate this review in the second half of 2025.
3.3.2.2.4	Information Compliance Office / ICT Services	Liaise with HR to organise staff training on digital records;	Consult with IT to identify staff training needs on digital records. Liaise with HR to organise training.	Discussion with DICT June 23. ICT to assess level of training required.
3.3.2.2.7	Information Compliance Office / VPGS	Expedite the planned exploration of options for maintaining a college archive and ensuring that access to this is fully compliant;p	Establish committee to explore options for maintaining a college archive and ensuring that access to this is fully compliant;	Terms of Reference have been drafted and are under review by the Vice-President of Governance & Strategy.
3.3.2.2.9	Information Compliance Office	Undertake a review of the storage infrastructure on the Thurles campus.	Visit Thurles campus to undertake a review of the storage infrastructure.	Met with Senior Academic Administrator, MIC Thurles in June 2024 regarding the initiation of a file review of storage files. This work will continue into 2025.

Table 5: Recommendations Not Actionable				
	Allocated To:	**Recommendation**	**Action Item**	**Reason for Non-Completion**
3.3.2.2.1	Information Compliance Office	Set the frequency of the review the Records Retention Schedule and enhance version control of it;	Consider appropriate frequency of review; Explore functionality with Privacy Engine around records retention schedule;	Superseded by Register of Processing Activities (RoPA) Project 2024. Records management conducted outside the Privacy Engine system.
3.4.2.1.1	Information Compliance Office	Integrate risks identified by PrivacyEngine into the ICRM Risk Register.	Work on integrating risks identified by PE into ICRM Risk Register. PE identifies specific risks for each office based on the DP log entered by DPC.	The Record of Processing Activities (RoPA) has reverted to excel format for ease of ICRM accessibility and maintenance for the Information Governance & Compliance Management (ICRM) team. The Excel method has been highly considered and is deemed the most appropriate and user-friendly method for all staff. Additionally, other Higher Education Institutions (HEIs) have agreed that using excel is the most practical solution, further supporting this decision. Risks are identified by ICRM and reported to offices as appropriate.