CORE DOCUMENTATION MANAGEMENT POLICY AND PROCEDURE

1

Core Documentation Category	Storage Location	Publication Location	Responsibility
Course Documentation Course Information Forms Course Handbooks	Academic Registry	VLE Intranet	Quality Manager
Institutional Documentation Guidelines Handbooks for External Persons	Academic Registry	College website VLE Intranet I	Quality Manager
Committee Terms of Reference Committee Minutes	Academic Registry	Intranet VLE	Quality Manager
Policies, Procedures & Regulations	Academic Registry	College website VLE Intranet	Quality Manager

Purpose

This policy aims to establish clear and compliant practices for the management, storage, and access of documentation at MIE . It ensures compliance with the **GDPR**, **MFHEA guidelines**, and local **Maltese data protection laws**. Additionally, this policy addresses institutional documentation practices related to user monitoring, document labelling, and long-term data retention.

2. Scope

This policy applies to all staff, students, and third-party service providers involved in the creation, management, or access of institutional documentation and records. This includes physical and digital documents, data related to students, staff, research, and outsourced activities such as recruitment and internships.

---

3. Roles and Responsibilities

- **Registrar**: Oversees the document management system, ensures compliance with GDPR, monitors user consent, and enforces the retention policies.
- **Data Protection Officer (DPO)**: Ensures that all data handling activities adhere to GDPR and MFHEA standards, including data security and privacy requirements.
- **IT Department**: Manages the digital systems, (e.g., SharePoint) hardware and software infrastructure contact used to store and track documentation, ensures secure access controls, and supports the automation of document retention processes.

- **Third-Party Service Providers**: Must adhere to the specific requirements outlined in Article 28 of the GDPR, including implementing institutional data security protocols, collaborating with the Data Controller, demonstrating compliance with the European Regulation within their organization, and ensuring the secure management of institutional data..
- **All Staff**: Are required to follow established documentation protocols, including labelling, storage, and access requirements.

Core Documentation Category	Storage Location	Publication Location	Responsibility
Course Documentation	Academic Registry, Digital Management System (e.g., SharePoint)	VLE, Intranet, Website	Quality Manager
Institutional Documentation	Digital Archives, Cloud Storage	College website, VLE, Intranet	Registrar, IT Department
Committee Terms of Reference	Digital Management System (e.g., SharePoint)	Intranet	Committee Chairs, Registrar
Policies, Procedures & Regulations	Digital Management System (e.g., SharePoint)	College website, VLE, Intranet	Registrar, Quality Manager

---

4. User Monitoring and GDPR Compliance

4.1 Monitoring Policies MIE shall not monitor or track user activity (e.g., students, staff) without obtaining explicit consent as per GDPR regulations. Monitoring includes any data collection via online platforms, internal systems, or third-party software.

4.2 Consent Requirements

- **Explicit Consent**: Before any monitoring activity begins, the Registrar's Office must collect signed consent forms from students and staff.
- **GDPR Compliance Form**: A GDPR compliance form must be signed by all users acknowledging their understanding of monitoring policies and their consent to being monitored.

4.3 GDPR Compliance for External Contractors

- Third-party service providers or contractors accessing institutional data must sign a **GDPR Contractor Compliance Form** in accordance with Article 28 that outlines their responsibilities and adherence to GDPR standards regarding the data they handle.
- External data processors must be formally appointed in accordance with Article 28 of the GDPR.

4.4 Responsibilities:

- **Registrar's Office**: Responsible for collecting and storing signed consent forms.
- **IT Department**: Ensures that monitoring tools and systems are aligned with GDPR principles.

---

5. Document Management and Labelling

5.1 Document Labelling Protocol All documents stored or circulated by the institution must be clearly labelled with the following:

- **Title/Subject**: A concise and descriptive title or subject heading.
- **Date**: Date of creation, submission, or modification.
- **Author(s)**: Full names of individuals responsible for creating or modifying the document.
- **Review Date**: Date by which the document should next be reviewed or updated.

- **Ownership**: Clear indication of document ownership within the institution.

5.2 Staff Training All staff handling documents will undergo regular training on document management best practices. This includes how to label, store, and retrieve documents securely.

5.3 Document Access Controls

- **Role-Based Access**: Only staff members with defined roles may access certain documents based on their job requirements. The **IT Department** will manage access control lists using the SharePoint system or equivalent document management system (DMS).

5.4 Responsibilities:

- **All Staff**: Responsible for labelling documents as per the institution's standards.
- **Registrar's Office**: Monitors document compliance with the labelling protocol and provides annual reviews.

---

6. Data Retention and Tracking

6.1 40-Year Retention Requirement MIE shall retain both physical and digital records for a minimum of 40 years in compliance with regulatory and accreditation requirements.

6.2 Digital Tracking System

- The **Registrar** is responsible for implementing and overseeing a **digital log sheet** or **document management system (DMS)** to track and archive records.
- This system must support automated indexing, retention, and retrieval of records, ensuring all documents are securely stored and accessible for audit purposes when required.

6.3 Physical Records Storage

- **Physical records** shall be kept in secure, fireproof storage, with limited access to authorised personnel. A detailed index of physical records will be maintained digitally to allow cross-referencing with electronic systems.

6.4 Responsibilities:

- **Registrar**: Ensures digital and physical records are retained in line with regulations and oversees the use of a digital tracking system.
- **IT Department**: Implements and supports the digital system, including data backup and archiving.

---

7. Document Access and Security

7.1 Access Controls

- **Role-Based Access Control** : Access to documentation is restricted based on staff roles, which will be defined and updated by the Registrar.
- **SharePoint Security Features**: The **IT Department** will integrate enhanced security measures such as multi-factor authentication (MFA) and encryption to safeguard sensitive information.

7.2 Outsourced Data Management

- **Third-Party Contractors**: All contractors with access to institutional data must sign **data security agreements** outlining their responsibility to comply with GDPR. These agreements will specify secure document handling practices and data protection measures.

7.3 Responsibilities:

- **IT Department**: Implements and manages access controls, including regular audits.
- **Third-Party Contractors**: Responsible for ensuring that their data access and storage procedures meet the security standards outlined in the institution's contractor agreements.

---

8. Auditing and Compliance

- **Annual Audits**: The **Registrar's Office** and **Data Protection Officer (DPO)** will conduct annual audits to ensure that all documentation management processes, including data retention, labelling, and access controls, comply with institutional policies and external regulations.
- **Training and Compliance Monitoring**: Regular training sessions will be held to ensure that staff and third-party contractors understand their responsibilities under this policy.

9. Breach Reporting

In case of a data breach or violation of GDPR principles, staff must immediately report the incident to the **DPO** and the **Registrar**. An investigation will be conducted, and necessary actions will be taken to rectify the breach and notify the relevant authorities (such as the Maltese Information and Data Protection Commissioner).

10. Policy Review

This policy will be reviewed and updated annually by the **Registrar** and **DPO** to ensure continued compliance with GDPR, MFHEA, and other regulatory requirements.

Document History:

- **Version**: 2.0
- **Effective Date**: 22/10/2024
- **Last Review Date**: 29/09/2023
- **Next Review Date**: 22/10/25

Appendix 1

Short Core documents front sheet template

Document Information

Document Control	**Details**
Policy Owner	
Document Number	
Version	
Effective Date	
Next Review Date	
Approval Date	
Approved By	
Distribution	

Document History

Version	**Date**	**Summary of Changes**	**Changes Approved By**
1.0		Initial policy creation	
2.0			
3.0			

Appendix 2

Long template for core document history

Document title				
Document date	*dd/mm/yy*			
Version number	*E.g. Drafts* *Revisions* *Approved versions v1.0, v2.0, v3.0*			
Author name and job title				
Circulation when approved and location(s) (Please Tick)		*Please Tick*		*Please Tick*
	Committee Members		*Confidential*	
	Staff			
	Students			
	Alumni			
	Public			
	Website/public intranet			
Other location/s	*e.g. Student Handbook/Programme Handbook*			
Review trigger date	*Ask Quality Manager for advice if required*			
	Yes	***No***	***Not applicable***	
Consultation with appropriate stakeholders	*e.g. Tick if consultation has been carried out and add references to evidence*			
Committee with final approval authority	*e.g. SMT*			
Date committee approval issued and minute reference	*Leave blank until approval has been given*			