MLI Information Management Policy and Procedures

Malta Leadership Institute

Version 1

2025

Dated Created	21st May 2025
Date updated:	Nil
Version:	1
Applicable to:	MLI Administration
Author:	Jesmond Friggieri
Location:	MLI, Birkirkara

Table of Contents:

MLI Information Management Policy and Procedures 1
1. Introduction 3
2. Document Control 3
3. The Fundamental Principle of the Policy 3
4. Policy Overview 4
3.1. Policy Purpose 4
3.2. Policy Scope 4
3.3. Policy Key Principles 4
3.4. Policy Review and Updates 4
5. MLI IT systems 5
5.1. IT Equipment and Platforms 5
5.2. Information access on the MLI website to the Public 5
5.3. Update and Backup of IT systems 6
6. Procedures 6
6.1. Procedures for Students 6
6.2. Procedures for Tutors/Lecturers 6
6.3. Procedures for MLI Staff 7
6.4. Additional Information Management Procedures 7
Appendix 1: IT Manager 8

1. Introduction

The aim of this policy is to establish robust standards and practices for managing information effectively and securely within the Malta Leadership Institute (MLI). It provides guidelines to ensure that information management practices comply with regulatory requirements, safeguard data integrity, confidentiality, and availability, and support efficient decision-making processes across all departments.

2. Document Control

Version	Section Responsibility	Authorisation	Date
1	IT Department	IT Manager/CEO	21st May 2025

3. The Fundamental Principle of the Policy

The fundamental principle guiding this policy is to ensure information is managed systematically, ethically, and responsibly, upholding the highest standards of data governance, security, and integrity. This ensures compliance with relevant laws and regulations and aligns with the MLI's values of transparency, accountability, and continuous improvement.

4. Policy Overview

3.1. Policy Purpose

The purpose of this policy is to:

- Define clear responsibilities and guidelines for managing MLI information.
- Protect information against unauthorized access, alteration, disclosure, or destruction.
- Promote efficient information retrieval and dissemination within authorized roles.
- Ensure regulatory compliance with data protection and privacy requirements.
- Support continuous improvement in information management practices.

3.2. Policy Scope

This policy applies to all MLI staff, students, contractors, consultants, and third-party vendors handling information managed or stored within the Institute's systems. It includes digital and physical data and covers all internal and external data-sharing activities, ensuring adherence under all operational circumstances.

3.3. Policy Key Principles

The following core principles underpin this policy:

1. **Confidentiality:** Information access is granted strictly based on roles and responsibilities.
2. **Integrity:** Data accuracy and consistency are maintained at all times.
3. **Availability:** Critical information is accessible when required by authorized personnel.
4. **Compliance:** Adherence to local and international regulations governing data protection and privacy.
5. **Accountability:** Clear responsibilities are established and communicated for managing information.
6. **Continuous Improvement:** Regular evaluation and improvement of information management practices.

3.4. Policy Review and Updates

1. This policy will be reviewed annually or whenever significant legislative, technological, or organizational changes occur. The IT Manager, in consultation with the CEO and relevant stakeholders, will oversee the review and update processes to ensure ongoing relevance and compliance.
2. Any updates shall take place according to changes that can take place from time to time. The IT Manager shall be responsible to register such changes and amend this Policy and Procedure.
3. When amendments take place, the IT Manager shall ensure that this shall never contradict the LCTS IT Policy and Procedures as established in LCTS Ltd Operational Policy and Procedure.

5. MLI IT systems

5.1. IT Equipment and Platforms

1. All computers and other IT related equipment are should be secured and well kept.
2. LCTS has the following IT systems in place:
   a. Email provider is Google Gsuite system, including Shared Drives
   b. Website of Malta Leadership Institute (https://maltaleadershipinstitute.com)
   c. Learning Management System (LMS) (https://maltaleadershipinstitute.edu20.org)
   d. PABX (telephone system) supported by Comsec.Ltd
   e. Vifto Accounting System for the Condominia Accounts (https://vifto.com)
   f. Dakar Online Salary system (www.salaroo.com)
   g. Turnitin (the plagiarism detection system which is integrated in the LMS)
   h. EBSCO – Online Library. This is only accessible through the LMS
   i. Zoom – this is platform used for online meetings and lectures.
   j. EU Projects and EU Funded Mobilities online systems:
      a. Application Dashboard: (https://webgate.ec.europa.eu/beneficiary-module/project/#/project-list)
      b. Erasmus+ Site Dashboard: (https://www.erasmus-dashboard.eu/account/login)
      c. Beneficiary Module: (Erasmus+ and European Solidarity Corps programmes)
3. Other IT systems for the benefit of the learners and staff might be put up from time to time. Staff using the systems will have to secure their access through logins and passwords provided by the systems accordingly. Passwords are to be kept safe and secure. The same applies to the systems that are accessible to the learners.
4. The IT Manager or the Administration officer responsible for certain systems shall ensure that all IT are up and running and payments to third parties are done in due time.

Though many systems are offered by third parties, however they have robust back systems and this is stipulated in terms and conditions of the purchase of the service.

5.2. Information access on the MLI website to the Public

1. The website is managed by a reliable third party.
2. The website has a content management system and it will be updated on a monthly basis with new information, if this is applicable.
3. Information on the website will include:
   - The selection criteria for the courses/programmes;
   - Intended learning outcomes of courses/programmes;
   - The qualifications awarded, including the EQF/MQF level and ECTS/ECVET learning credits;

- The teaching, learning and assessment procedures used;
- The pass rates;
- Further learning opportunities available to the students.

4. The person responsible of the website will also update from time to time and where applicable information about policies and procedures for courses.
5. Feedback from tutors and students will be considered to improve the information published on the website.
6. The course Co-ordinators are responsible to check that the information on the website is correct and accurate,

5.3. Update and Backup of IT systems

1. Systems that can be backed up manually and this will be done by the IT Manager person to back-up all the course work once a week and keep it secure in a folder within the LCTS/MLI IT systems unless the relevant platforms such as Google Drive have enough robust back up.
2. Backups will be saved both on the cloud system (google drive) used for everyday work and also on the server. This ensures that in case of any failure in equipment there are recent copies of the services and data on the cloud.

6. Procedures

6.1. Procedures for Students

1. Students must protect their login credentials and never share passwords.
2. Students should immediately report any suspected breaches of their accounts or misuse of information.
3. Students should regularly backup their coursework and important data using the designated cloud storage provided (Google Drive).
4. Students must adhere to the guidelines provided when using the LMS and other digital platforms.

6.2. Procedures for Tutors/Lecturers

1. Tutors/Lecturers must maintain confidentiality when accessing and using student data and course information.
2. Regular backups of course content, assessment records, and relevant academic documents must be conducted using cloud storage (Google Drive) and institutional servers.
3. Tutors/Lecturers must update course content regularly on the LMS and ensure accuracy and completeness of information.

4. Any suspected unauthorized access or information breach must be immediately reported to the IT Manager.

6.3. Procedures for MLI Staff

1. Staff must secure all IT equipment assigned to them and regularly update passwords according to policy guidelines.
2. Staff must back up important operational and administrative data weekly to both cloud storage and institutional servers.
3. Any new software or digital platform implementation should be authorized by the IT Manager and CEO.
4. Staff should routinely verify information published on the MLI website for accuracy and report any discrepancies.
5. Staff must promptly inform the IT Manager of any suspected security breaches, software malfunctions, or data integrity issues. The IT Manager shall follow the LCTS & MLI Data Protection Policy and Procedures.

6.4. Additional Information Management Procedures

1. All sensitive documents, physical or electronic, must be clearly marked and securely stored, with access restricted to authorized personnel only.
2. Disposal of physical documents containing sensitive or confidential information must be performed through shredding or other approved secure methods.
3. Regular training and awareness sessions on information security and data protection must be conducted for all MLI community members.
4. Any requests for data extraction or analysis must follow formal authorization processes, ensuring compliance with data protection regulations.
5. Information sharing with external parties requires signed confidentiality agreements and adherence to institutional guidelines on data privacy.
6. Regular audits of information management practices should be performed to assess compliance and identify areas for improvement

Appendix 1: IT Manager

Role Purpose: The IT Manager/Officer ensures the effective and secure management of MLI's information technology infrastructure and systems, in alignment with the Institute's information management policies and compliance requirements.

Key Responsibilities:

- Oversee the development, implementation, and monitoring of IT security protocols.
- Manage backups, disaster recovery plans, and ensure data integrity and confidentiality.
- Regularly review and update information management practices and policies.
- Coordinate staff training on IT and information management procedures.
- Ensure regulatory compliance with data protection laws and standards.
- Respond to and resolve IT security incidents and breaches.
- Liaise with external vendors and stakeholders on IT-related matters.
- Advise the senior management team on technology investments and system upgrades.

Reporting: The IT Manager/Officer reports directly to the CEO.