IML IT POLICY

Istituto Marangoni London
May 2025

Version Control Statement

Version			
Document title	IML IT Policy		
Document approved by	Finance and Resources Committee 03 AY 2024-2025		
Approval date	08.05.2025		
Date for review			
Amendments since approval	Detail of revision	Date of revision	Revision approved by

TABLE OF CONTENT

1 Introduction & Scope

1.1 This policy outlines the appropriate use of IT and communication systems at Istituto Marangoni London. It applies to all employees, faculty, visitors, contractors, and third parties who access the School's IT infrastructure.

1.2 The purpose is to promote effective and secure operations while ensuring responsible technology use across academic and administrative environments. This policy operates in alignment with the Information Security Policy, Cybersecurity & Business Continuity Policy, and wider IMHQ and GGE frameworks.

2 Policy Authority and Review

2.1 This policy is issued under the authority of the Senior Management Team and maintained by the ICT Department. It is reviewed annually or following any significant changes in technology, operations, or regulatory frameworks.

3 Responsibilities

3.1 The ICT Department is responsible for day-to-day implementation and support. All staff are expected to uphold the standards within this policy and contribute to a culture of digital security, reporting concerns promptly.

4 Equipment & Company Accounts Use

4.1 Users are accountable for the equipment and accounts issued to them. All devices must be kept secure, with passwords protected and devices locked when unattended.

Users must not:

- Use shared credentials or allow others to access their account.
- Connect unauthorised hardware or install unapproved software.
- Modify, delete, or tamper with system files or configurations.

4.2 Software installations must be licensed and approved by ICT. Shadow IT, including the use of unauthorised platforms or apps, is prohibited.

5 Email & Communication

5.1 All use of School-provided email accounts must comply with the IMHQ Email Policy and be limited to professional purposes. Users must:

- Avoid forwarding School email to personal accounts.
- Refrain from sending confidential data unencrypted.
- Use the School signature and disclaimer on all messages.

5.2 Emails are a formal communication channel and must reflect the standards of professionalism and accuracy required by the School.

6 Internet Usage

6.1 Internet access is primarily for School-related purposes. Minimal personal use is permitted if it does not interfere with responsibilities or breach policy. The following are not permitted:

- Accessing illegal or offensive websites.
- Using unapproved platforms for storing or transmitting School data.
- Streaming or downloading non-work-related content that may consume significant bandwidth.

7 Monitoring

7.1 All systems are subject to automated and, where appropriate, manual monitoring. Monitoring supports cybersecurity, legal compliance, and the protection of institutional assets. Access to personal communications will only occur under strict protocols with appropriate authorisation.

8 Prohibited Use

Users must not:

- Distribute discriminatory, defamatory, or offensive content.
- Engage in unauthorised access, data breaches, or cyberattacks.
- Use AI or large language models to upload School, staff, or student data (e.g., OpenAI, Gemini) without prior authorisation from ICT.

Breaches of this policy may result in disciplinary action, including dismissal.

9 Incident Reporting

All users must immediately report:

- Phishing attempts or suspected compromise.
- Lost or stolen devices.
- Any unauthorised access or potential data breach.

Reports should be directed to the ICT Department and line manager. Timely reporting is essential and failure to do so may result in disciplinary action.

10 Account Lifecycle Management

User accounts are managed according to IMHQ's IT Offboarding Procedure. Key points include:

- Accounts are disabled on the user's final day.
- Autoreply is activated; email forwarding is not permitted.
- Accounts are deleted 30 days after departure unless required for legal or business continuity purposes.
- Access reviews occur periodically for all active accounts.

11 Training and Awareness

11.1 All staff must complete induction and refresher training covering security awareness, acceptable use, and incident procedures. ICT may run additional campaigns in response to emerging risks.

12 Relationship to Other Policies

This policy should be applied alongside:

- Information Security Policy
- Cybersecurity & Business Continuity Policy
- Data Protection Policy
- IMHQ Data Classification Policy
- Email Policy
- Staff Handbook

Where overlap occurs, the most specific or stringent rule shall take precedence.