istitutomarangoni

ISTITUTO MARANGONI LONDON
IT ACCEPTABLE USE POLICY FOR STUDENTS

istitutomarangoni

Version Control Statement

Version	1.0
Document title	IT Acceptable Use Policy for Students
Approved by	Senior Management Team
Approval date	11 September 2024
Date for review	July 2025
Amendments since approval	

IT Acceptable Use Policy

1. Introduction

1.1. This IT Acceptable Use Policy outlines the acceptable and unacceptable use of Istituto Marangoni London's IT resources, including computers, networks, software, and internet access. The policy aims to protect the integrity of our IT systems and ensure that students use these resources responsibly and ethically.

1.2. It should be read in conjunction with related IML policies and guidelines including:

- Data Protection Policy
- Student Privacy Notice
- Student Handbook
- Student Code of Conduct and Disciplinary Procedure
- Safeguarding Policy
- Dignity at Work and Study Policy

1.3. All students are expected to be aware of this policy and comply with its provisions as required by the Student Code of Conduct.

2. Scope

2.1. This policy applies to all students of Istituto Marangoni London who have access to the institution's IT resources.

2.2. Members of staff and other personnel should refer to the IML ICT Policy.

3. Purpose

3.1. The IT acceptable use policy sets out students' responsibilities and IML's expectations for the use of its IT resources. It aims to ensure that these resources are used appropriately, maximising their availability for legitimate purposes by maintaining security and minimising misuse.

3.2. IT resources, including hardware such as computers and printers, software, email and user accounts are provided to students on the condition that they are used for acceptable purposes only in accordance with the guidance set out in this policy.

4. Roles and Responsibilities

Role	Responsibilities
All students	Complying with the IT Acceptable Use Policy. Reporting any known breaches of this policy to the ICT Manager.
School Director	Overall responsibility for IML's information security
ICT Manager	Operational responsibility for information security at IML Responsible for implementation of this policy
Registrar	Oversight of student disciplinary action resulting from misuse of IT resources
Senior Management Team	Approving and reviewing the Student IT Acceptable Use Policy

5. General Principles

5.1. IML IT resources, including IT user accounts, are provided for students to support their learning. The School does not prohibit students from reasonably using IML IT resources for personal business outside of their studies, proving that they abide by the principles of this policy.
5.2. IML email accounts are the main channel of written communication with and between staff and students. Students should ensure that they check their IML email on a regular basis and use this email address to contact IML staff.
5.3. Students must respect the rights of other users and refrain from actions that disrupt or interfere with others' use of IT resources.
5.4. Students must comply with all applicable laws, rules, regulations, and institutional policies while using IT resources. Failure to comply will be deemed as misuse under this policy and may lead to initiation of disciplinary proceedings.
5.5. Use of IML IT resources for personal financial gain is not permitted.
5.6. Confidential information should be stored securely and careful consideration should be given to maintaining confidentiality when sharing sensitive information.

6. Expectations for Acceptable Use

6.1. Students are responsible for maintaining the security of their accounts and devices. This includes using strong passwords, logging off when not in use, not sharing login credentials and ensuring that personal devices are protected by suitable anti-virus software.
6.2. Students who accidentally disclose their IT password or other security information must report this to the ICT Manager at the earliest opportunity.
6.3. The terms of the various software and data licence schemes under which IML provides access to certain systems and resources must be complied with. Where relevant students' attention will be drawn to the rules associated with these schemes before access is granted.
6.4. Students should have regard to the intellectual property rights of third parties, particularly when downloading, forwarding and using materials that are copyrighted or contain branded materials, examples include logos, pictures, text, video files, and icons.
6.5. Any IML owned IT equipment borrowed from the School must be returned at the time agreed and any stored data removed.
6.6. Where use of IT resources could contravene this policy but is required for legitimate learning purposes, permission should be sought from the Research Ethics Group or relevant Programme Leader as appropriate.
6.7. Students should be familiar with the online safety guidelines (appendix A) and adhere to these when working online using IML IT resources.

7. Unacceptable Use

7.1. The following is an indicative list of the types of activity or behaviour that are considered unacceptable (other activities may be considered unacceptable depending on the specific context in which they occur):

- Using IML IT resources in any way that is fraudulent, offensive, obscene, racist, malicious defamatory or libellous
- Accessing, creating, or distributing content that is illegal, harmful, or inappropriate, including but not limited to pornography, hate speech, and violence
- Using IT resources to carry out any acts which could incite or promote extremism including, but not limited to, accessing websites or sharing material that might be associated with extremist or terrorist organisations
- Engaging in any form of harassment, bullying, or threatening behaviour online (known as 'cyberbullying')
- Breaching a third party's intellectual property rights (e.g. licences, copyright, trademarks)

- Sending/posting unsolicited advertising or spam
- Attempting to gain unauthorised access to information or to alter, damage or delete such information (e.g. 'hacking')
- Using IT resources to disrupt the work of others or deny them access to such resources
- Using IT resources for commercial activities or personal gain without explicit authorisation from the institution.
- Installing or reconfiguring unauthorised software on IML owned devices
- Deleting or modifying system files
- Connecting any device that extends IML's network without authorisation from the ICT Manager
- Attempting to monitor the use of IML IT resources (including use of key logging or screen capture affecting other users), or attempting to access system logs
- Disassembling, modifying or disposing of IT equipment without authorisation
- Using IT resources to engage in plagiarism, cheating, or any form of academic misconduct

8. Monitoring and Privacy

8.1. Students should be aware that in order to ensure that acceptable use of its IT resources is maintained in accordance with this policy and with UK law, IML monitors IT resource usage. This includes monitoring network traffic, email, file storage and usage logs.

8.2. Web filtering is used to screen out harmful content (including adult content, pornography, hate speech and child sexual abuse materials) and help protect students from online harm.

8.3. While the School respects students' privacy, it cannot guarantee absolute confidentiality of data stored on its IT resources. The School reserves the right to monitor and/or record communications as appropriate under the following circumstances:

- To establish facts to ascertain compliance with IML regulations and policies
- In the interests of national or international security
- To comply with lawful requests for information from government and law enforcement agencies
- To prevent or detect a crime
- To investigate or detect unauthorised use of IML's systems
- To secure effective system operation

8.4. Any requests to monitor and/or record communications and data will be subject to permission from the School Director or Registrar. All monitoring shall be in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

8.5. System administrators may copy user data or disable user access in order to preserve evidence until such time as an investigation can be conducted.

9. Breaches of this Policy

9.1. Failure to comply with this policy may result in disciplinary action in accordance with the Study Code of Conduct and Disciplinary Policy. In severe cases this may include exclusion from the School and in the case of suspected criminal acts, the incident will be reported to the Police.

9.2. Any suspected breaches of this policy should be reported immediately to the ICT Manager. Any attempt to conceal a breach or suspected breach may result in disciplinary action.

9.3. IML has a student complaints procedure and safeguarding reporting procedures that enable any member of the School to raise formal concerns about a student's actions, including those associated with IT use.

10. Policy Review

10.1. This policy will be reviewed and updated every three years by the School's Senior Management Team, or sooner in response to relevant legal, statutory or regulatory changes.

Appendix 1: Staying Safe Online

When using social media and online services, think about how your actions might impact you and those around you, both online and offline.

Below are some tips for navigating the online world in a way that protects your safety and wellbeing.

- Remember to review and adjust privacy and safety setting when you download new apps or buy new technology.
- Use the service provider's tools to manage your digital footprint and remember content posted online could be shared publicly by anyone.
- Avoid sharing personal information when you're chatting or posting online.
- Only open messages, files or images from people you know and trust.
- Learn how to report inappropriate content to service providers and use blocking and deleting tools. Any member of the public can report terrorist content they find online through the GOV.UK referral tool. The Action Counters Terrorism campaign provides more information on this.
- Contact Student and Academic Services if you have any concerns about radicalisation and the University's community, or online content associated with the University.
- Protect yourself against fraud and financial scams and do not give your bank details to anyone you don't know and trust

Useful resources

- SWGfL's test my privacy to check their privacy settings on various platforms and you can use their social media checklists to keep up with the safety features on popular social media platforms.
- The UK government's Cyberaware website includes advice on how to stay secure online.
- You can report harmful online content here: https://reportharmfulcontent.com/
- The UK Safer Internet Centre – publishes resources to help children and young people stay safe online and provides guidance to support those experiencing online abuse https://saferinternet.org.uk/
- The Internet Watch Foundation works to identify and remove online child sexual abuse images and videos and has an anonymous reporting form on its website: https://www.iwf.org.uk/