Information Technology Acceptable Use Policy

Version 1.1

Policy Author	Anthony Satariano	Designation	Head QA	Dept.	QA Dept.
Policy Reviewer	Joanne Grima	Designation	CEO	Dept.	N/A
Policy Approver	QAC	Effective Date	25/09/2018		

1   Purposes

1.1   This Acceptable Use Policy applies to all users of Information Technology (IT) resources owned or managed by the Institute for Education (IfE). Individuals covered by the policy include (but are not limited to) the IfE's staff, persons on a contract for service, course participants, past course participants, educators attending courses at the IfE's premises, guests, and external individuals.

1.2   This Policy is intended to provide a framework for such use of the IfE's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

1.3   IT resources include all the IfE's owned, licensed, or managed hardware and software, the IfE's assigned user accounts on the portal or other third-party software accessed via the portal (Turnitin®, Emerald Publishing, ProQuest and Alexander Street), and use of the IfE's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

2   Scope

2.1   The IfE on seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to course participants and staff of the IfE.

3   Introduction

3.1   The IfE provides Information Technology resources to a large and varied group of educators. In accordance with the IT Acceptable Use Policy, all users have the responsibility to use these resources in an effective, efficient, ethical, and legal manner. Ethical and legal standards that apply to IT resources are based on the standards of common sense and courtesy that apply to any shared resource. The IfE provides IT resources with the stipulation that IT users act as good citizens and that they contribute to creating and maintaining an open community of responsible users.

4   Principles of Acceptable Use

4.1   This Policy is based on the following principles:

- Users must use the IfE's IT Resources in a responsible, safe and lawful manner.
- Users must respect the integrity of computer systems, communication devices and networks to which they have access.
- Users must respect the integrity of the data to which they have access.
- Users must store and process the IfE's data in compliance with the Course Participants' Records Policy and the Employee Records Retention and Access Policy and the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act (Cap 586).
- Users must follow any standards and guidelines (including those set out in this Policy) relating to the use of the IfE's IT Resources.

5   Roles and responsibilities

5.1   Each User is responsible for:

- Complying with this Policy and all other relevant policies and procedures;
- Ensuring all passwords assigned to them are kept confidential;
- Reporting all breaches of this Policy to ife@ilearn.edu.mt.

6   Acceptable Use

6.1   In making acceptable use of resources, users covered by this policy must:

- Use IT resources only for authorized purposes.
- Protect their User ID(s) and system from unauthorized use. Each individual is responsible for all accesses to the IfE's information resources and technology by their User ID(s) or any activity originating from their system. An individual's User ID and password act together as their electronic signature.
- Access only information to which they have been given authorized access or that is publicly available.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.

- Restrict personal use of the IfE's information resources and technology to incidental, intermittent and minor use that is consistent with applicable law and IfE Policy

7 Non-Acceptable Use

7.1 Users must not use the IfE's IT resources to:

- Other than in the course of performing their duties, knowingly access, download or distribute illegal or inappropriate material, including material that is in any way pornographic, obscene, abusive, racist, libellous, defamatory or threatening.
- Engage in any form of bullying or other behaviour which is illegal or likely to cause harassment to others.
- Use social media to degrade, bully or intentionally offend staff, course participants or other users or use these tools to bring the reputation of the IfE into disrepute.
- Gain unauthorised access to the account, systems or equipment of any third party - attempts at 'hacking' may result in criminal prosecution in Malta or elsewhere.
- Use another user's credentials to log into his/her account.
- Perform any activities which contravene the law, or the destination country in the case of data being transmitted abroad.
- Undertake commercial activities or to otherwise further commercial objectives which are not a part of the user's work/studies in the IfE.
- Breach the copyright, patent or other intellectual property rights of any person, by downloading unlicensed software or other unauthorised materials.
- Breach the data protection or other privacy rights of any person. Please refer to the IfE's Data Protection Policy.
- Use of the IfE's systems or resource to facilitate plagiarism or cheating in exams or assignments.
- Access, modify, or interfere with computer material, data, displays, or storage media belonging to the IfE or another user, except with their permission.
- Connect unauthorised equipment to the IfE's network.
- Load or execute unlicensed software or other material on the IfE's IT resources where this is likely to breach the licensing conditions or other Intellectual Property rights.
- Knowingly introduce any virus, malware or other destructive program or device into the IfE's systems or network.
- Store sensitive or confidential IfE data on personal devices.

8   Related policies

- Course Participants' Records Policy
- Employee Records Retention and Access Policy
- General Data Protection Regulation (GDPR) (EU) 2016/679
- Data Protection Act (CAP 586)
- CCTV Policy and Procedures
- Data Protection Policy

9   Version history

Originator	Version	Date	Changes Done
QA Dept	1.0	25/09/2018	Initial Release
QA Dept	1.1	30/04/2024	Updated links