IT Systems Acceptable Use Policy

Contents

1. Introduction

1.1 This Policy provides a framework for the acceptable use of the ICMT's Information Technology (IT) to ensure that it can be used safely, lawfully and equitably.

1.2 The Policy comes into force upon the commencement of employment with the ICMT, or for students, by the authorised user logging in for the first time.

2. Scope

2.1 This Policy applies to the use of all physical and digital assets of the ICMT. (See Note 1)

2.2 This Policy applies to all users of the ICMT's IT systems irrespective of the user's location. (See Note 2)

3. Governance

3.1 You are bound by the ICMT's Data Protection and Information Security policies, standards and guidance. You are also required to act according to this Policy and all relevant laws and contractual obligations or licensing conditions relating to the services you are using.

3.2 When using IT (including social media), all users must observe the requirements of the ICMT's regulations, standards and policies, and current law. (See Note 3)

3.3 You are required to always apply to the highest standard of ethics.

3.4 When accessing services from another jurisdiction other than the UK, you must abide by all relevant data protection laws, including the Data Protection Act 2018. This also includes those applicable to the service location and where the data are being collected, stored, processed or otherwise controlled by the ICMT. (See Note 4)

4. Compliance

4.1 You must comply with this Policy and any reasonable written or verbal instructions issued by people with delegated authority. If you feel that any instructions are unreasonable or are not in support of these regulations, you may appeal to the Operations Manager.

4.2 You must not attempt to youse the IT facilities without the permission of the ICMT.

5. Acceptable use

5.1 You may not undertake any activity that may reasonably be regarded as unlawful or potentially so. This includes but is not limited to the following:

- Breaking the law.
- Not abiding by the ICMTs, or any third party regulations, policies and guidelines.
- Allowing anyone else to use your digital credentials (e.g. your login username and password).
- Disguising your online identity.
- Attempting to obtain or use anyone else's online identity.
- The Computer Misuse Act also covers unauthorised access to systems or data. It may result in a breach of the law, and those gaining such unauthorised access may result in a significant fine and/or imprisonment.

5.2 Do not put the ICMT's facilities at risk by:

- Loading, installing or using unauthorised software on the ICMT equipment.
- Attempting to remove approved security software.
- Attempting to execute malicious files or code on any device owned by the ICMT.
- Creating, downloading, storing or transmitting unlawful material, or material that is indecent, offensive, violent, threatening or discriminatory.
- There will be other instances where the ICMT has provided you with software or resources. You shall only use software and other resources in compliance with all applicable licenses, terms and conditions.
- Use of services for personal activities is permitted, provided that this does not infringe any of the ICMT's regulations, policies or procedures. This is a privilege that may be withdrawn at any point. (See Note 5)

- The Counter-Terrorism and Security Act 2015 places a duty on the ICMT to have the need to prevent people from being drawn into terrorism. Accordingly, users must not access terrorist material whilst using the ICMT's IT services as it is a criminal offence.
- The ICMT must report to the authorities any confirmed attempts to access illegal terrorist or other criminal information.
- No personally subscribed-to service belonging to staff (personal email accounts or personal social media accounts) may be used for work purposes. No controlled data of the ICMT may be sent to or stored in such personal accounts.

6. Monitoring

6.1 The ICMT will comply with lawful requests for information from Government and law enforcement agencies. The ICMT monitors and records the use of its IT facilities for:

- Ensuring business continuity.
- The effective and efficient planning and operation of the IT facilities.
- Investigation of alleged misconduct.
- Accessing files or email in an employees/student's absence.
- The detection and prevention of infringement of policies or standards.

7. Infringement

7.1 Any infringement of this Policy or third party regulation may result in disciplinary action and may, in addition, be subject to penalties under civil or criminal law.

7.2 The ICMT reserves the right to recover from you any costs incurred due to your infringement.

8. Explanatory notes

8.1 This section offers examples and is intended to relate to your everyday use of the IT facilities and the Acceptable Use Policy.

8.2 Where examples are given, these represent only some of the most common circumstances encountered. The list is not intended to be exhaustive.

Note 1

Physical and digital assets of the ICMT. This includes bus is not limited to:

a) IT hardware that the ICMT provides, such as printers, desktop computers, laptops and tablets.
b) The ICMT network and connected components.
c) Software that the ICMT provides, such as operating systems, office application software, web browsers etc. Including software that the ICMT has arranged for you to have access to, for example, special deals for staff and students on commercial application packages.
d) Data that the ICMT acquires, processes, provides or arranges access.
e) Online services arranged and authorised by the ICMT.
f) IT credentials, such as your use of your ICMT account login and password.

Note 2

The regulations apply to anyone using the ICMT's IT facilities. This means more than students and staff. It could include:

a) Visitors to the ICMT website.
b) The ICMT applicants.
c) People accessing the ICMT's online services off-campus.
d) External partners, contractors or agents based onsite or offsite and accessing the ICMT's services and systems.
e) Visitors using the ICMT's digital infrastructure, such as Wi-Fi.

Note 3

You must be familiar with the ICMT's general regulations and policies. Your online behaviour is subject to UK law, even if those are not related to IT.

Note 4

If you are using services hosted in a different part of the world, you will also be subject to the local laws of that country.

Note 5

You may currently use the IT facilities for personal use provided that it does not breach any policy or regulation of the ICMT and does not prevent or interfere with other people using the facilities for ICMT purposes.

Document control

Document Title	IT Systems Acceptable Use Policy
Document Category	General Policies
Version	1
Status	Approved
Author	Operations
Date of current version	February 2022
Date of next review	February 2023
Document location	ICMT website
Communication plan	Email link to website included in offer and on the student portal.