Policy Title:	MIE Staff & Students Code of Conduct for Use of IT Systems
Description:	The user agrees to abide by all licence agreements associated with use of software and data that have been entered into by Marino Institute of Education (MIE) with the licence providers, and the terms and conditions of use therein. Software provided by MIE may be used only as part of the user's duties as a student or staff member of MIE, for educational purposes.
Author (Position):	Director of IT and eLearning
Version:	2
Approved By:	MIE Governing Body
Policy Approval Date:	January 2019
Date of Next Policy Review:	April 2023 (or as necessary)

MIE Staff & Students Code of Conduct for Use of IT Systems

1 Context

Marino Institute of Education (MIE) computing resources are provided to facilitate a person's work as a member of staff or as a student of MIE. These resources can be used for educational, training and research purposes. Computing and network resources must not be used for any commercial or significant personal use.

2 Purpose

2.1 Software provided by MIE may be used only as part of the user's duties as a student or staff member of MIE, for educational purposes.

2.2 The user agrees to abide by all licence agreements associated with use of software and data that have been entered into by MIE with the licence providers, and the terms and conditions of use therein.

3 Policy

3.1 In order to use the network and computer facilities of MIE, a person must first be 'authorised' to be on the network. Registration on the network grants authorisation to use some, or all, of the computing and network facilities of MIE.

3.2 During registration and/or IT induction, a username and password are issued to each student. These are for the exclusive use of that student for the duration of their studies in MIE.

3.3 Unauthorised use must not be attempted, or made, of computing or network privileges and resources allocated to an individual.

3.4 The user is responsible for any and all activities carried out under their username. The password associated with a particular username must not be divulged to any other person. Passwords used must adhere to good password practice, as outlined at IT Induction. Further information about good password practice can be viewed at https://www.tcd.ie/itservices/security/tips-good-practice.php.

3.5 Attempts to access or use any username which is not authorised to the user are prohibited, and such attempts may be subject to breach of the Criminal Damage Act, 1991. Such breaches will be investigated in full by members of the IT Team and can result in sanctions, such as revocation of IT privileges, in the first instance.

3.6 No person shall jeopardise the integrity, performance or reliability of Institute computer equipment, software and other stored information. In this context, "software" is taken to comprise programmes, routines, procedures and their associated documentation which can be implemented on a computer system, including personal computers and workstations. The integrity of MIE's computer systems may be jeopardised if users do not take adequate precautions against malicious software (e.g. computer virus programmes). Suggestions on good practice for protection against malicious software are available at https://www.tcd.ie/itservices/security/tips-good-practice.php.

3.7 Existing norms of behaviour apply to computer-based information technology just as they would apply to more traditional media. The ability to undertake a particular action does not imply that it is acceptable. Examination of any files on the computer of a colleague is equivalent to examining their filing cabinet. Seeking to find unprotected files on a multi-user system falls into a similar category. Whilst it is possible to send via the computer communications which may be offensive, obscene or abusive, such behaviour is not acceptable.

3.8 The user undertakes not to use any MIE computing or network resources to make use of or publish material that is obscene, libellous or defamatory or in violation of any right of any third party.

3.9 If emails are being sent to express personal as opposed to Institute views, users should put in a disclaimer to that effect in their message.

3.10 No user shall interfere or attempt to interfere in any way with information belonging to another user. Similarly, no user shall make unauthorised copies of information belonging to another user.

3.11 Any software, data or information which is not provided or generated by the user personally and which may become available through the use of computing or communications resources shall not be copied or used without permission of MIE, or the owner of the software, data or information.

3.12 The user undertakes not to infringe any copyright of documentation or software.

3.13 The user undertakes to comply with the provisions of the Data Protection Act, 1988, European Communities (Data Protection) Regulations, 2001, European Communities (Data Protection and Privacy in Telecommunications) Regulations, 2002, Data Protection Directive 95/46/EC, Data

Protection Act, 2018 and General Data Protection Regulation (GDPR) EU 2016/679 and other relevant legislation.

3.14 The user must not undertake any actions that bring the name of MIE into disrepute.

3.15 The user may use approved MIE links to other computing facilities which they are authorised to use. When using external facilities, the user must also abide by their rules or code of conduct.

3.16 Persons who break this code of conduct may find themselves subject to MIE's Disciplinary Policy and/or criminal procedures, as considered appropriate.

4 Responsibility

4.1 The Director of IT & eLearning, and members of the IT Team have responsibility for this Policy.

4.2 The Director of IT & eLearning, is responsible for the implementation of this policy with respect to MIE.

5 Related Documents

5.1 Data Protection Act, 1988

5.2 European Communities (Data Protection) Regulations, 2001

5.3 European Communities (Data Protection and Privacy in Telecommunications) Regulations, 2002

5.4 Data Protection Directive 95/46/EC

5.5 Data Protection Act, 2018

5.6 General Data Protection Regulation (GDPR) EU 2016/679

5.7 MIE Privacy Policy

5.8 MIE IT Security Policy

5.9 Accessible Information Policy

5.10 The Library of MIE Data Protection Statement and CCTV Policy

5.11 MIE Website(s) Terms of Use

5.12 MIE Policy on Management of MIE Website

5.13 MIE Website Cookies Policy

5.14 Guidelines for External Examiners on European General Data Protection Regulation 2018

5.15 MIE GDPR Data Processing Agreement with External Examiners

5.16 Guidelines on GDPR for Research Purposes

5.17 MIE Policy on Social Media and Social Networking

5.18 Disciplinary Policy