

Marino Institute of Education, Colaiste Mhuire has very strict guidelines on the use of email, internet and IT systems generally. You are required to familiarise yourself with and adhere to these policies and procedures. This document provides specific instructions on all aspects of the usage of these systems. However, if you are in any doubt please contact a member of the IT Team for further clarification.

The staff member/student should use this document as a general introduction to the topic of Computer Security and Usage, and to the approach taken by Marino Institute of Education, Coláiste Mhuire to ensure all our information assets are safe and secure. This policy applies to all information systems, regardless of the department they are in or the technology that is used. Standards, procedures and guidelines exist to support the implementation of legislation that governs the use of IT, and this simplified policy covers the main areas of concern. This policy identifies the expected behaviour and responsibilities for every person involved with using MIE information and communication systems.

For further detailed analysis of any specific query relating to topics covered in this policy, please contact a member of the IT Team who can help clarify the position in relation to the legislation, and liabilities created therein.

**Purpose:**

1. To provide a secure and productive computing environment for MIE
2. To increase awareness of computer security amongst staff and students of MIE
3. To increase the awareness of their responsibilities when using MIE resources
4. To provide a guideline for protecting valuable information resources from theft, damage and unauthorised access or change
5. To increase the awareness of confidentiality, copyright and freedom of information when dealing with sensitive MIE information and records.

**MIE's Expectation of Users:**

1. Users must use user-ids/passwords for MIE's specified purpose, and must not use any other user's id/password with or without that user's permission

2. Users must protect their user-id and password from unauthorised use, as they are responsible for all activities, legal or otherwise, associated with their user-id
3. Electronic communication facilities (such as email) should not be used to send fraudulent, harassing, obscene, threatening or other unlawful messages
4. Users may not create, send or forward multilevel marketing letters (jokes, chain letters, pyramid selling schemes, requests for sensitive user information)
5. Users must not attempt to modify, duplicate or remove computer equipment, software, or peripherals without proper authorisation.

Violations of these conditions of acceptable use may, after due process, result in any of the following:

- The suspension of computing privileges
- Disciplinary action in line with MIE's disciplinary procedures

Monitoring tools are in place for email, internet and phone usage. Logs of all calls made, emails sent and received etc., from our gateway are retained in separate servers, and users should be aware of this.

**Virus Protection:**

In order to limit the spread of computer viruses, MIE has invested heavily in our anti-virus protection. Even though we have virus protection, there is always a risk of a new virus of which we have no prior notification.

As we increasingly look to outside resources for information and email, it is important we be aware of virus infection and the damage it can do. Introduction of viruses and other contaminants can occur through a variety of sources:

- Third party laptops are not permitted access to our network. Before they are connected to the system, they should be screened by a member of the IT Department.
- Email from any party, whether a trusted associate or casual acquaintance
- CDs from magazines and periodicals
- Software introduced into or used on the system by an outsider who has access to the system
- Software used at home on an infected system
- Software purchased from a vendor who has an infected production system
- Infected software from bulletin boards or the internet

Anti-virus updates are sent automatically to all networked computers. Please note the following:

- Any CD/USB sticks of uncertain or dubious origin should be brought to the IT Dept., for checking before use, otherwise you run the risk of infecting your PC and consequently, the network, with a virus
- Do not load any software to your system without getting the prior permission of the IT Dept., as they must certify all software is virus free
- Any virus alert or detection should be reported to the IT Dept. immediately where the event can be logged, the source found and contacted and the media dis-infected. Do not use the terminal any further until the IT Dept has had a chance to investigate.
- To reduce the chances of getting a virus, please refrain from sharing CDs/USB sticks
- Loading of games and non- approved software onto terminals is strictly prohibited
- All software loaded on MIE terminals is fully licensed. If the IT Dept., finds unauthorised software, it will be removed immediately and may result in disciplinary action being taken with the individual concerned.

**Email Usage Policy:**

In order to ensure we get the best value from the email system, in terms of speed and ease of access, there are a number of standards that should be adhered to.

Email is suitable for short communications, making arrangements and sending documents that could be printed off by a recipient. Your email account is for business/student related activity only.

Email should not be used

- To send confidential information
- To send membership or student data (Data Protection Act forbids this)
- To try and discuss complex or lengthy issues. If necessary, such matters should be put in a MS Word document and sent as an attachment.
- To send chain letters, jokes etc. The issuing or forwarding of such mail items can be considered a disciplinary matter.

MIE strives to maintain an educational environment free of harassment and sensitive to the diversity of its users. Therefore, MIE prohibits the use of computers and email in ways that are disruptive, offensive to others or harmful to morale. For example, the display or transmission of sexually explicit images and/or cartoons are not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off colour jokes, or anything that may be construed as harassment or showing disrespect for others. Email may not be used to solicit others for commercial ventures, religious or political causes, outside organisations, or other non-business related matters.

MIE is bound by legislation such as the Child Trafficking and Pornography Act, 1988 for mandatory reporting of any person or persons or systems accessing inappropriate materials.

MIE uses an automatic mail spam filtering system. This programme is configured to stop all viruses, programmes, images, profanities and other words associated with spam. If a genuine email is stopped by the spam filter, it will be released to the user on request to a member of the IT Dept.

To ensure compliance with this policy, users are reminded that email usage is monitored.

**Legal Position:**

It should be borne in mind, that contents of both internal and external emails are discoverable in legal proceedings. Information in relation to student personal details is specifically mentioned, and can be “discovered” due to Freedom of Information legislation. Therefore, the normal precautions that you would take in regard to “publishing” should be preserved. If you would not write it in a normal letter, then it should not go in an email. A good rule of thumb is as follows

“If you are happy to send something that anyone can alter and read, then send it in an email”.

**Internet Usage:**

MIE has internet access through its broadband, ISDN and leased line links. Many of the internet's activities are for recreational and private use and are unrelated to MIE's business. For that reason, access to certain services on the internet can be restricted.

The risks to MIE from internet usage are even greater than those associated with email, hence the need for stricter rules.

- MIE internet connections are intended for the activities that support MIE's business or the professional development of student users. Those who, in the opinion of the IT Dept, have abused this may have their computing privileges revoked.
- Users have the responsibility for internet access under their log in/password and hence have responsibility for illicit/illegal use of that password, with or without their consent
- Information used, or presented, on the internet should not violate the terms and condition of the various Copyright Acts and Data Protection legislation.
- The internet should not be used for personal gain or profit, to post, download or circulate messages and materials that contain inappropriate, obscene, inflammatory, intimidatory, harassing, defamatory, disruptive, pornographic, sexist, racist or otherwise offensive language, materials, images or files

You use the internet as an agent of MIE, and must therefore maintain the highest degree of professionalism at all times. All communications with external organisations must constantly demonstrate this professionalism.

MIE reserves the right to inspect a user's access to ensure compliance with MIE policies, and legal obligations are being maintained, therefore internet usage is monitored.

**Copyright Legal Position:**

MIE recognises the legal right of copyright, and our position is to protect the rights of owners of intellectual property. Users of MIE systems should be aware that copyright law applies to materials accessed or published on the internet. Materials on the internet should be considered to be the subject of a copyright, unless specifically mentioned that it is not subject

to copyright. Most specifically, users must not put any copyrighted materials (eg. Video, music, software etc.) on web pages or published materials for dissemination, without prior permission from the copyright owner, or appropriate authority.

The primary source of information in relation to copyright law is “Copyright and Related Acts, 2000” and a useful website to understand copyright generally can be viewed at [www.whatiscopyright.org](http://www.whatiscopyright.org)

4 things to consider before using “materials”:

- The intended use (is it “not for profit” educational purpose, for example)
- The nature of the copyrighted work (different mediums are treated differently, eg. Music )
- The quality and quantity (use only what is necessary)
- The danger of financial damage to the copyright holder

You must not

- Prejudice the interests of the copyright holder
- Make multiple copies
- Copy for another person where you reasonably believe that other person will make multiple copies of this material, and make such material available to more than one person

You may copy if

- You hold the copyright
- The copyright has expired (usually 50 or 70 years after death of the author/copyright holder)
- You have permission from the copyright holder
- The copying falls within the concept of “fair dealing” and is for research, private study, criticism or review (with acknowledgement).
- The concept of “fair dealing” applies to almost all works, including electronic resources
- Often, specific licence agreements associated with electronic resources impose further proprietary restrictions associated with specific publishers/suppliers.

End./