



Waterford Institute *of* Technology

INSTITIÚID TEICNEOLAÍOCHTA PHORT LÁIRGE

ACCEPTABLE USAGE POLICY AND GUIDELINES FOR THE INSTITUTE'S E-MAIL.

Contents

ACCEPTABLE USAGE POLICY AND GUIDELINES FOR THE INSTITUTE'S E-MAIL	1
1. Status of the document	2
2. Why WIT needs an E-mail policy.....	2
Legal liability	2
Workplace harmony and the Image of the Institute	2
Network congestion & down time	3
3. Implementation	3
Acceptable Use Policy and Guidelines for the Institute's E-mail.....	4
Policy Implementation	6
GLOSSARY OF TERMS	7

1. Status of the document

- This policy was developed as a WIT Partnership Committee project in consultation with staff Unions, WITSU and Management. It was approved by Governing Body on and became a formal policy of the Institute.
- The policy is an attempt to balance the rights of individual Users to privacy and confidentiality with the need to protect the organisation and other Users from e-mail misuse.
- The next major review of the policy will take place in March 2006 unless changes in legislation or technology require an earlier intervention.
- This Policy applies to all Users of the WIT e-mail e.g. staff, students, auxiliary services, visitors, and consultants, in all locations from which WIT e-mail may be used and from all servers connected to the WIT LAN.

2. Why WIT needs an E-mail policy

- a) E-mail has brought huge benefits to WIT in terms of improved communications, enabling Institute staff and students to communicate promptly, efficiently and effectively with colleagues inside the organisation and clients, customers and suppliers externally. For most of us, e-mails have almost replaced office memos, newsletters and other forms of routine paper communications. In many cases, it is more convenient to send e-mail to an individual or group than to call them individually. Chat and instant-messages are a natural extension of this concept.
- b) The advent of e-mail has made communication very convenient and instant. However, with the convenience comes an element of risk. People using e-mails tend to forget that they are also a form of official documentation. Also, with the available technology, an e-mail that seems to be “deleted” may be traceable. As the industry matures, and the usage of e-mail permeates to all the different functional areas of our business, it is becoming clear that the consequences of exchanges that Users make over the Internet using Institute systems put both the Users and WIT at risk.
- c) The purpose of this document is to inform Users about these threats, legal, interpersonal and technological, and to advise all Users on the acceptable use of e-mail required for workplace harmony and maintaining the good image of the Institute.
- d) All Users have the responsibility to use the Institute’s computer resources in an efficient, ethical, effective and lawful manner

Legal liability

- e) WIT is legally responsible for all the information transmitted on or from its systems. The organisation therefore has a duty to provide all Users with clear information and guidelines for acceptable use. E-mail records have the same legal standing as letters and disclosure of e-mail messages may be required under Freedom of Information legislation and attachments are subject to copyright laws. It is important that all Users are aware of these risks.

Workplace harmony and the Image of the Institute

- f) E-mail is provided by WIT to facilitate communications relating to the business of the Institute. The excessive use of e-mail for social or leisure purposes or for the distribution of inappropriate information is time wasting and can be a source of annoyance to others. In some extreme cases communications may be regarded as offensive or be a cause of harassment. An e-mail policy can help stop this by increasing awareness of the possible impact of e-mail on the recipient.

Network congestion & down time

- g) Spam and personal (mis) use of e-mail can cause network congestion since they are not only unnecessary, but tend to be mailed to a large list of recipients and often include large attachments such as mp3, executable or video files that Users do not zip. Viruses are another important area of concern. If a virus hits the WIT system this can cause network congestion or even down time. Again it is important that all Users are aware of these technical issues and the best way to do this is to attend one of the training courses offered regularly by Computer Services.

3. Implementation

- h) It is important that all Users understand that this policy has been developed for the benefit of everyone and that violations of this policy may result in the activation of disciplinary procedures.
- i) While legal advice to the Institute states “*Users should not, under any circumstances, have an expectation of privacy in anything of a personal nature that they create, store, send or receive via the Institute’s computer resource*” WIT recognises that the principles of academic freedom and shared governance, freedom of speech and privacy of information hold an important place in the ethos of the organisation. WIT therefore tries to find a reasonable balance between the expectation of privacy, which it normally affords to paper and telephone conversations, and the special capacity of E-mail for misuse.
- j) A clear system for dealing with policy infringements is included at the end this document.

Acceptable Use Policy and Guidelines for the Institute's E-mail.

1. E-mail access and usage are provided to Users by WIT primarily for carrying out the business of the Institute. Both the nature of e-mail and the public character of the Institute's business make e-mail less private than Users may anticipate. Users are encouraged to keep private use to the minimum.
2. An e-mail, whether business or personal, may constitute an official WIT record and disclosure may be requested under the Freedom of Information Act.
3. WIT e-mail may not be used for private commercial activity such as advertising products or services, promotions, the deliberate transmission of destructive programmes or viruses, chain letters or political canvassing and lobbying.
4. Users should be aware of the legal framework applying to e-mail and should take great care to avoid creating liabilities for themselves or for WIT. For example e-mail from WIT can be used to form binding legal contracts if the individual sending it has actual or apparent authority to do so. Also, if an employee were to give professional advice in e-mail, WIT will be liable for the effect of the advice that the recipient or even third party, reasonably relies upon. If an employee of WIT were to receive a confidential mail from someone and by accident forward it to the wrong person, the employee, and therefore WIT, could be liable.
5. While WIT respects the rights of Users to free expression, Users should reflect deeply before they use the Institutes e-mail to advance their personal, social and political views or to distribute jokes or gossip. The Institute's community is multi-cultural and multi-national and such e-mails can provoke arguments or cause embarrassment or offence to others. It is important to remember that harassment complaints are based on the impact on the recipient rather than the intention of the sender and that different people have different reactions to and tolerance to the tone and content of e-mails. Sending an e-mail from WIT's system should be regarded as comparable to sending a letter on WIT- headed paper. The content should therefore be appropriate and professional at all times.
6. It is strictly forbidden to use the Institute's computer resources to access or transmit offensive images or text such as pornography, inappropriate screensavers or other material. Any unauthorised attempt to access another persons account or the use of another person's password is prohibited. The use of WIT's computer resources for such purposes or in such a manner is totally inconsistent with the code of conduct and ethical standards required of all WIT Users.
7. WIT, in general, cannot and does not wish to be the arbiter of the contents of e-mails. While it cannot fully protect Users from receiving e-mails they may find offensive, it strongly encourages Users to communicate professionally and with courtesy. In composing e-mails take great care not to make defamatory or careless remarks directly or by innuendo. Remember how easy it is to misaddress an e-mail and send it to the wrong person and the ease with which the recipient can circulate, forward and store it. As a general rule it is good practice not to forward person-to-person e-mails without the consent of the sender. Remember that backup copies of e-mails may exist either archived centrally or saved on the recipient's hard-disc, even if you have deleted them from your own computer.
8. Users are advised to limit e-mail messages to individual Users whenever possible. The practice of copying e-mails to many people can cause distress and embarrassment to the main recipient. This could be interpreted as threatening or intimidating behaviour by the sender. If you need to communicate with many Users, you should try to use a targeted mailing list. If you want something done, address the e-mail only to the User who should be responsible – if you send it to several people, there is a good chance none of them will act! Indiscriminate use of the "all-staff" distribution list is strongly discouraged. Messages that would be of interest to everyone should be posted on the WIT intranet.

9. Users should be aware of the dangers of distributing or receiving malicious software including viruses, Trojan horses and worms. If a User sends or forwards an e-mail that contains a virus, this will have serious implications for WIT. While WIT implements a good virus checker that blocks viruses entering and leaving it via e-mail, you should carry out an additional check of all attachments received from external sources. If you receive a virus alert from anyone other than Computer Services at WIT, do not circulate it to all staff as the vast majority of virus warnings are hoaxes in themselves and their intention may be to simply clog up systems through such reactions.
10. Users should be aware that attachments are subject to copyright rules (an outline of these can be found on the WIT Library web site). They should also take care about sending very large attachments such as photographs and ensure that they do this in the most economical manner possible.
11. E-mail Users should be aware that there is no guarantee that the e-mail received was in fact sent by the purported sender. Senders can use forged e-mail addresses: this is very common for Spam. If your name is selected, then it looks like the Spam came from you. In case of doubt, receivers should check with the purported sender to validate authorship and authenticity. It will be regarded as serious offence for a WIT User to employ a false identity when sending an e-mail.
12. Where proxy access to a generic or group account is required a proxy access form must be completed and sent to Computer Services. The onus is on both parties to review this arrangement and inform Computer Services when staff leave an area.

Policy Implementation

1. There is a strong onus on Users to ensure they understand the technical and legal framework in which they operate. In order to keep up to date with this changing technology, everyone should avail of the training opportunities offered regularly by the Institute.
2. If you have any concerns about computer viruses, you should inform Computer Services immediately.
3. If you are distressed by any inappropriate or offensive messages by e-mail, you should inform your Head of Department or Line Manager as soon as possible. You should save the e-mail electronically and print a hard copy for records that may be required as evidence for subsequent investigations or disciplinary actions.
4. In the case of disturbing, indecent, obscene, sexist or racist content, you may, if you wish, contact one of WIT's equality support persons and invoke the provisions of the Institute's *Dignity and Respect at Work and Study Policy*.
5. Any reported infringements of *WIT's Acceptable Usage Policy and Guidelines for the Institute's E-mail* will be investigated and appropriate action will be taken in accordance with the Institute's agreed grievance, disputes and disciplinary procedure.
6. An investigation of a complaint may involve the inspection, monitoring or disclosure of e-mail records. Unless there are legal reasons for not doing so e.g. a court order, the e-mail account holder will be notified in writing that a decision has been made to undertake such a search and will be provided with the documented reasons for this decision. Decisions must be authorised by a named decision maker (see glossary of terms).
7. If the e-mail account holder wishes to appeal a decision to inspect, monitor or disclose his / her e-mails, s/he must do this within the specified period, given in the letter of notification. An internal reviewer who has not previously been involved in the case, must consider this appeal. The appeals officer shall decide if the search is justified or not and this decision will be implemented.
8. Inspection, monitoring or disclosure may be undertaken without consent in emergency circumstances where time is of the essence and where there is a high probability that delaying action might result in
 - significant bodily harm,
 - significant property loss or damage,
 - loss of significant evidence or
 - other significant liability to WIT or to members of the Institute's community.
9. Emergency action without the Users consent can only be authorised by a WIT decision maker. The least level of perusal of contents and the least action required to resolve the emergency will be authorised.
10. Technical and support staff in computer services may need to monitor transmissions periodically to ensure the proper functioning and security of the network. They are bound to respect the privacy of Users within the framework of this policy and must not seek out, reveal or use contents which are not germane to the purpose of their search.
11. Should the Institute be required to disclose e-mails in response to Freedom of Information requests, the above procedure of notification, except in emergency, and the right to appeal will apply.

GLOSSARY OF TERMS

Attachments:	A file attached or included with an e-mail message. Some e-mail systems can only send the message that you type on the screen, but others can include a file with the message.
Decision Maker	A Decision Maker is the person who decides in the first instance what information is to be released to or withheld from the requester. These duties have been delegated by the Director according to Section 4 of the FOI Act, to Heads of Department and Central Services Managers.
E-mail:	Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses.
Executable:	A file format that the computer can directly execute. Humans cannot read executable files.
Forward:	To send on a received e-mail to another person or group without editing it.
Hard copy:	A print out of data e.g. an e-mail stored on a computer. It is considered hard because it exists physically on paper, whereas a soft copy only exists electronically.
Internal Reviewer	An Internal Reviewer under FOI, is the person who decides what information is to be released or withheld from the requester should the requester appeal the initial decision. This Internal Reviewer must be of a ranking grade higher than that of the Decision Maker [see above]. These duties have been delegated by the Director according to Section 4 of the FOI Act to Heads of School and Heads of Function.
LAN:	A computer network limited to the immediate area, usually the same building or campus.
Mailing list:	A (usually automated) system that allows people to send e-mail to one address, whereupon their message is copied and sent to all of the other subscribers to the mailing list.
mp3:	File format used for the compression of audio files.
Proxy:	Someone, other than the account holder who has been granted access rights to an e-mail account
Server:	A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a web server software, or to the machine on which the software is running, e.g. e-mail server.
Spam:	An inappropriate attempt to use a mailing list or other networked communications facility as if it was a broadcast medium by sending the same message to a large number of people who did not request it.
Trojan horse:	A computer program is either hidden inside another program or that masquerades as something it is not in order to trick potential Users into running it. For example a program that appears to be a game or image file but in reality performs some other function. A Trojan Horse computer program may spread itself by sending copies of itself from the host computer to other computers, but unlike a virus it will (usually) not infect other programs.
Virus:	A chunk of computer programming code that makes copies of itself without any conscious human intervention. Some viruses do more than simply replicate themselves, they might display messages, install other software or files, delete software or files, etc. A virus requires the presence of some other program to replicate itself. Typically viruses spread by attaching themselves to programs and in some cases files, for example the file formats for Microsoft word processor and spreadsheet programs allow the inclusion of programs called "macros" which can in some cases be a breeding ground for viruses.
Working Days	Days when WIT is open for business - not just teaching terms.
Worm:	A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.
Zip:	A popular data compression format. Files that have been compressed with the Zip format are usually called Zip files.