

Regulations on the Usage of the Internet from the University.

The purpose of this policy is to ensure the proper use of the University's Internet access by its employees and students. Internet access is a tool that is provided for authorized use by the members of the University community primarily for the business of the University and users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Violation of this policy may result in disciplinary action, including possible termination of employment and/or legal action.

In normal circumstances all access to the Internet is via a proxy server. Only in exceptional cases will employees or students be given direct access.

1. Usage of the Internet.

1.1 Internet access is provided to staff and students to enable them to pursue their work as an employee or student of the

University of Limerick. The Internet must not be used for commercial or personal gain.

1.2 Staff and students may use the Internet for personal use provided that it:

- does not incur additional cost to the University
- does not prevent the employee from attending to and completing work effectively and efficiently
- does not preclude others with work-related needs from using the resources,
- does not result in any unauthorised personal profit to the individual
- does not expose the University to legal liability
- does not involve or constitute an illegal activity

2. Copyright.

2.1 Staff should be careful to ensure that any software, files or any other document is not copied or re-transmitted in breach of copyright or other intellectual property rights.

3. Privacy Protection.

3.1 Regardless of the level of protection provided for Internet communications, confidentiality cannot be assured. Confidentiality might be compromised, for example, by law or policy, including this Policy, by unintended redistribution, or by the inadequacy of current technologies to protect against unauthorised access. Therefore, users should exercise extreme caution in using Internet communications to transmit confidential or sensitive matters.

3.2 Staff should also be aware that the University keeps a log of all accesses to the Internet - including the identifier of the computer accessing the internet, the identification of the site being accessed and the amount of data transferred. These logs are kept by ITD for 12 months. The University could be requested to reveal such logs in the event the law being broken or by a Court order. The logs are kept to analyse statistically the University Internet traffic.

3.3 The University shall only permit the disclosure of sites accessed by an individual without their consent:

- when required by and consistent with law,
- when there is **substantiated reason** (as defined below) to believe that violations of law or of University policies have taken place.

3.4 This disclosure will be authorised in advance and in writing by two members of the University's Deans' Council. This authority may not be further re-delegated. Requests for such non-consensual access must be submitted in writing. Authorisation shall be limited to the least perusal of contents and the least action necessary to resolve the situation. The responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other University policy, notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

4. Unavoidable Inspection.

4.1 Users should be aware that, during the performance of their duties, personnel who operate and support internet communications facilities need from time to time to monitor transmissions or observe certain transactional information to ensure proper functioning of University internet communications facilities and services, and on these and other occasions might inadvertently observe the contents of internet communications. Except as provided elsewhere in this Policy or by law, they are not permitted to: hear, see, or read the contents intentionally, observe transactional information where not germane to the foregoing purpose, or disclose or otherwise use what they have seen, heard, or read.

4.2 One exception to the foregoing paragraph is the occasional need for systems personnel to inspect the contents of internet communications and transactional records. Such unavoidable inspection of internet communications is limited to the least invasive level of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal and confidential information, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable internet communication to its intended recipients. Except as provided above, systems personnel shall not intentionally search internet communications records or transactional information for violations of law or policy but shall report violations discovered inadvertently in the course of their duties. Access is restricted to named systems personnel and their names are lodged with the Human Resources Office.

5. Prohibited Usage.

5.1 The following use of the Internet conflicts with University policy; breaches of this policy should be reported to the Director, ITD.

- The creation and exchange of files/messages that are illegal, offensive, harassing, defamatory, obscene or threatening or that are in conflict with the University Code of Conduct in the Use of Computer Facilities or national legislation.
- The unauthorised exchange of proprietary information, trade secrets or any other privileged, confidential or sensitive information.
- The unauthorised creation and exchange of advertisements, solicitations and viruses.
- The creation and exchange of information in violation of any copyright laws.

5.2 Individuals in breach of this policy are subject to the University of Limerick's disciplinary and/or criminal procedures.

6. Definitions.

Substantiated Reason: Reliable evidence or information indicating that violation of law or of University policies probably has occurred, as distinguished from rumour, gossip, or other unreliable evidence.

Approved by Executive Committee March 2001