INSTITUTE OF TECHNOLOGY TALLAGHT

Computer Security and IT Usage Policy

Preamble

The Institute of Technology Tallaght is committed to the provision of a high standard of computing and network facilities. The purpose of the policy is to ensure the proper use of IT Tallaght's computer and network systems. It is also the purpose of this policy to ensure that every staff member and student is aware of the procedures in place to ensure fair processing of data. This policy should be read in conjunction with the already published policy on the use of e-mail and the HEANet Acceptable Usage Policy . In addition to protecting the integrity of the Institute's computer and network systems, this policy is also designed to protect the good name and reputation of the Institute, its staff and students.

Main Issues The Institute is obliged to protect its staff and students, and any third party to whom the Institute owes a duty of care, from improper or illegal use of its computer and network systems. As well, the Institute is obliged to take all reasonable steps to prevent its systems being attacked by viruses, unwanted spam and malicious hackers. To this end the Institute has installed a variety of security measures including access control and firewalls. It has also installed software to block access to illegal or unacceptable websites. Furthermore it is continually increasing its security measures on foot of both legal and technical advice in the light of the ever-increasing threat presented by external attacks. Minimal and incidental private usage of Institute systems which is not excessive and does not interfere with work obligations and which complies with Institute policy is permissible. While all data on Institute systems are Institute data and potentially accessible under Freedom of Information legislation, the Institute as a data controller complies with data protection legislation. Staff and students have the right to view all personal information held about them within the terms of data protection legislation. The capacity to monitor traffic over the Institute systems to ensure defence against external attack and the filtering of access to material which does not comply with policy is a feature of the Institute's overall security arrangements. Insofar as personal data, whether generated by the Institute or by the staff and students themselves, is concerned, the Institute will only process such data fairly and within the requirements of legislation. The Institute is registered as a data controller under the Data Protection Acts, 1998 and 2003, and has specified that personal data generated by staff or students is maintained both on individual staff PCs and on back-up servers. Overall responsibility for the security of the Institute's computer and network systems resides with the Computer Services Manager.

Hardware Only authorised hardware may be connected to the Institute's networks or use any of the Institute's licensed software. Hardware includes PCs, laptops, notebooks, PDAs, removable storage devices, printers, scanners, cd writers/rewriters and any peripheral device which is capable of interacting or communicating with the Institute systems.

Software Only authorised and licensed software approved by the Institute may be installed on Institute approved devices and network systems. The use of the following types of software is prohibited:

- Peer –to- Peer (P2P) and Instant Messaging software may not be installed on any PC connected to the Institute's network.
- ♦ Application software capable of attacking security systems may not be installed on any device whether or not connected to the Institutes network. Downloads

- Although much illegal or unacceptable material is filtered by the Institute's systems, staff and students are reminded that the downloading or attempted downloading of illegal material is viewed by the Institute as a grave breach of discipline.

- The downloading of MP3 or music files is expressly prohibited. Staff and students should not connect any device to the Institute's systems containing such files.

Administration Rights Administration rights are only given subject to specific controls. All persons with administration rights must sign specific undertakings as may be defined or amended from time to time by the Institute.

Appeals The Institute has established an appeals committee to review applications for access by staff to blocked internet sites. This committee is guided by current legal and technical advice in making its determinations.

Major Emergencies In view of the ever-increasing threat posed by malicious hackers and destructive viruses the Institute wishes it to be known that it reserves the following absolute rights in cases of emergency which threaten the security of the Institute's systems and reputation.

- To shut down all or part of its network
- To deny service to any members of staff or the student body
- To take whatever pre-emptive action is necessary to ensure compliance with all legal requirements

In the light of continuing technical and legal developments and in the interests of governance and best practice the Institute will keep its security policy under review and issue an amended policy/policies as appropriate.

Revision 1 Effective 12th February 2004