


Acceptable Usage Policy		
	3IT13	File Location:
		Current Revision: 01
		Approved by: TMG 8 January 2001
	3IT13	Document Owner: IT Manager
		Document Level: 3

Acceptable Usage Policy

Revision History

Revision	Date	Revision Description DCRT#	Originator
01	02 September 03	Conversion of OP100	Lisa Whelan
02	28 September 06	Change document name	IT Manager
03	06 October 08	Added section to cover Laptop security & Operating systems.	IT Manager

1 Purpose

The Institute wishes to implement an Acceptable Usage Policy for all of its' computer facilities and resources.

2 Scope

While self-discipline will be expected and encouraged the following specific provisions shall apply both to staff and students of the Institute.

3 Acceptable usage

- 3.1 Only registered students and staff of the Institute can use the Institute computer facilities. Access to facilities of the Institute by members of the public is strictly forbidden.
- 3.2 Users must accept individual responsibility for the personal resources (i.e. Home Directory and mailbox) allocated to them. It is expected that Users will adhere to reasonable security standards. As a matter of course, Users should not share passwords, leave passwords lying around in plain text, or otherwise compromise the security of their personal resources.
- 3.3 The User is responsible for the consequences of any use of the services provided by Institute. The Institute will not be liable for any indirect or consequential loss, damage, cost or expense of any kind howsoever including (without limitation) loss or corruption of data.
- 3.4 The Institute's services may not be used for any activity, which contravenes the laws of Ireland, or any other applicable jurisdiction.
- 3.5 Users may not use the Institute's services to seek to gain unauthorised access to the Institute's facilities, services or resources or to the facilities, services or resources of connected networks.
- 3.6 Users may not use the Institute's services to engage in activities, that waste the Institute's resources (people, networks, computers and financial).
- 3.7 Users may not use the Institute's services to engage in activities that cause, or are liable to cause, disruption or denial of service to other Users.
- 3.8 Users may not use the Institute's services to create, host, or transmit offensive or obscene material, or engage in activities, which would cause offence to others on the grounds of race, creed or sex.
- 3.9 Users may not use the Institute's services to create, host, or transmit material, which is designed to cause annoyance, inconvenience or needless anxiety to others.
- 3.10 Users may not use the Institute's services to create, host, or transmit material, which is defamatory.

- 3.11 Users may not use the Institute's services to create, host, or transmit material, which infringes the copyright of another person or organisation.
- 3.12 Users may not use the Institute's services to engage in activities that infringe the proprietary rights of software.
- 3.13 Users may not use the Institute's services to engage in activities that compromise the privacy of others.
- 3.14 Users may not use the Institute's services to engage in activities which would destroy the integrity of computer based information.
- 3.15 Users may not use the Institute's service to transmit unsolicited commercial or advertising material either to other Users or to other organisations connected to other networks, if the transmission of such material causes, or is likely to cause, annoyance.
- 3.16 The Institute's services are not intended for resale. Resale of services without making specific arrangements with the Institute is not permitted.
- 3.17 Users may not use the Institute's services for unsuitable purposes, including the use of unsuitable, offensive or obscene resource names.
- 3.18 Failure to comply with these regulations may be considered an act of gross misconduct and may result in initiation of disciplinary procedures that may include verbal warnings, restriction of services available or, in cases of gross misuse, dismissal or expulsion.

4 Internet access

- 4.1 Access to the Internet is provided to support genuine educational and research goals. Incidental personal use is not prohibited, but should be kept to a minimum. It is the responsibility of each individual to comply with the Institute policies governing information security and appropriate use of computer resources. The Institute logs all activity on its Internet proxy servers and has the right to monitor Internet use. Suspected misuse is subject to investigation and may result in disciplinary action, including verbal warnings, restriction of services available or, in cases of gross misuse, dismissal or expulsion.
- 4.2 When one accesses the Internet an electronic fingerprint is recorded. Internet mail, unless encrypted, can be viewed or accessed by unauthorized individuals who monitor Internet traffic. The Institute is committed to protecting its information assets and the Institute network.
- 4.3 Examples of inappropriate and unacceptable use of Internet access are:
 - any use expressly prohibited by Institute policy
 - extended use for personal or non-Institute business
 - operation of a personal business or activity intended to achieve personal financial gain

- making Institute confidential information available to unauthorized individuals, inside or outside the Institute
 - sending, forwarding, browsing, exporting from, or importing into the Institute any materials that are or could be, in any manner whatsoever, considered to be pornographic, obscene, offensive (whether from a sexual, racial, political, religious or any other perspective), defamatory or of a criminal or subversive nature.
 - any use that could bring the Institutes name into disrepute.
 - loading of material likely to be considered offensive by the public on the Institute website
 - linking through the Institute website to unacceptable sites
- 4.4 The content of all Web pages hosted via the Institute's computer facilities must be approved in advance by the Registrar or their nominee.
- 4.5 The Institute reserves the right to record the location of all Internet sites accessed and to share this information with relevant authorities.

5 Network use

- 5.1 The Institute Network may be used only for lawful purposes.
- 5.2 Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or intellectual property right used without proper authorisation, and material that is obscene, defamatory or constitutes an illegal threat.
- 5.3 The user acknowledges that the Institute is unable to exercise control over the content of the information passing over the Institute Network. Therefore, the Institute is not responsible for the content of any message whether or not the posting was made by an Institute employee or student.
- 5.4 The Institute Network may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.
- 5.5 The user may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").
- 5.6 Without prejudice to the foregoing, the Institute considers that any application that overloads the Institute Network by whatever means will be considered as making profligate use of the Institute Network and is as such NOT allowed.
- 5.7 Users who violate systems or network security may incur criminal or civil liability. The Institute will fully co-operate with investigations of suspected criminal violations, violation of systems or network security under the leadership of law enforcement or relevant authorities.

6 System and network security

- 6.1 Violations of system or network security are prohibited, and may result in criminal and civil liability. The Institute will investigate incidents involving such violations and will involve and will co-operate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:
- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network;
 - Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network;
 - Attempts to use or join non-ITB supplied equipment on the Institutes LAN.
 - Attempts to use or join non ITB supplied operating system software or derived application software on the Institutes LAN.
 - Interference with service to any user, host or network including, without limitation, mail-bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
 - Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.
- 6.2 If approached with complaints relating to any of the above violations, the Institute will co-operate and assist the Police and law enforcing bodies with their investigations in order to bring such misuse and violations to an end.

7 E-Mail

- 7.1 It is explicitly prohibited to send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements).
- 7.2 It is also explicitly prohibited to allow others to send unsolicited bulk mail messages either directly or by relaying through the Users systems. For the avoidance of doubt, users must ensure that their systems cannot be relayed through. Users may not forward or propagate chain letters nor malicious e-mail.
- 7.3 A User may not solicit mail for any other address other than that of the user, except with full consent of the owner of the referred address.
- 7.4 Posting of material not needed by the recipient, particularly to E-mail distribution lists is strongly discouraged.
- 7.5 Users are prohibited from forging e-mails.
- 7.6 Users are prohibited from reading, deleting, copying or modifying e-mail messages of other users without permission.

- 7.7 Users are prohibited from sending pornographic or obscene messages or other messages in violation of Institute policies concerning discrimination or harassment.

8 Laptops

- 8.1 By taking possession of an Institute provided laptop, the user accepts responsibility for safeguarding the equipment while it is in the users care. The following precautions must be adhered to:
- 8.1.1 Only authorized officers are entitled to remove laptop computers from the confines of the campus. Members of the management team are provided with laptop computers to facilitate off-campus work. All other staff members must be provided with written authorization from a manager or borrow the equipment from the Library, before removing a laptop computer from the campus.
 - 8.1.2 Officers who are provided with Laptop computers must ensure that appropriate file security and encryption procedures are employed to safeguard confidential data. Details of file security measures employed must be provided to the IT Support Department. [Passwords, Encryption key, biometric override etc.]
 - 8.1.3 Where the data contained in laptop files or applications may potentially be used to identify staff, students or other personal data. It is the responsibility of users to ensure that appropriate security and encryption is employed.
 - 8.1.4 When a laptop is taken off site the user is responsible at all time for its safe keeping.
 - 8.1.5 When not in use, laptops must be stored in a locked drawer or cabinet. Where possible the office door should be kept closed as a minimum and ideally locked.
 - 8.1.6 When authorized officers take a laptop home, the user must ensure that all reasonable security measures are employed to safeguard the equipment. That is, all doors are secured when you go out and the home security system is activated.
 - 8.1.7 When staying in a hotel, ensure that the laptop is locked in a room safe where available. If no safe is available, lock the laptop in a suitcase when exiting the room.
 - 8.1.8 When going through airport checkpoints, the user must keep the laptop in sight at all times. It is helpful to tape your business card to the laptop to help identify the laptop in airport security.

- 8.1.9 When travelling by car, lock the laptop in the boot or in a hidden secure compartment when you park.
- 8.1.10 Do not use the Laptop in locations that might increase the likelihood of damage.
- 8.1.11 Keep food and drinks away from the Laptop.
- 8.1.12 Laptop computers must always be carried in a padded case, specifically designed for the purpose.
- 8.2 If the laptop is stolen during an assault, or if it is damaged or stolen despite your having followed the guidelines listed above, it will be replaced with another laptop. In this case the Institutes' general operating budget will pay any portion of the cost not covered by the Institute's insurance.
- 8.3 If the laptop is damaged or stolen and the above procedures were not followed, your department will assume responsibility for the insurance deductible.
- 8.4 Damaged or stolen equipment must be reported as soon as possible to the: IT Manager, IT Support Department. He will report stolen equipment to the Gardai or other appropriate authority for insurance claim and replacement. If the theft occurred outside ITB, you must report the theft to the local police and obtain a police report.

9 General

- 9.1 The Institute reserves the right to take such action as it deems in its' discretion to be appropriate against any user who violates any conditions of the Computer Usage Policy. Such actions may include the suspension, interruption, restriction or termination of service as considered appropriate by the Institute. In such circumstances, the Institute will take such steps which it considers reasonable and appropriate. However, should it become necessary to invoke disciplinary procedure the Institute will follow the steps outlined in The Institute Disciplinary Procedures.
- 9.2 Indirect or attempted violations of policy, and actual or attempted violations by a third party on behalf of an Institute staff member or student shall be considered violations of this policy.
- 9.3 The Institute reserves the right to modify this policy at any time, effective upon posting of the modified Policy.

//ends