Acceptable Use Policy

Introduction

The University seeks to promote and facilitate the proper and extensive use of computing/IT in the interests of learning and research. Whilst the traditions of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students and staff of the University.

This Acceptable Use Policy is intended to provide a framework for such use of the University's computing/IT resources. It applies to all computing and networking facilities provided by any department or section of the University. It should be interpreted such that it has the widest application, in particular references to Computing Services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of a computing service.

1) Purpose of Use

University computing resources are provided to facilitate a person's work as an employee or student of the University, specifically for educational, training, administrative or research purposes.

Use for other purposes, such as personal electronic mail or recreational use of the WorldWide Web or Usenet News, is a withdrawable privilege not a right. Any such use must not interfere with the user's duties or studies or any other person's use of computer systems and must not, in any way, bring the University into disrepute. Priority must always be granted to those needing facilities for academic work.

Commercial work for outside bodies, using centrally managed services requires explicit permission from the Head of Computing Services; such use, whether or not authorised, may be liable to charge.

2) Authorisation

In order to use the computing facilities of the University a person must first be authorised. All members of the University should apply to Computing Services for registration. Registration to use University services implies and is conditional upon acceptance of this Acceptable Use Policy, for which a signature of acceptance is required on joining the University.

The registration procedure grants authorisation to use the core facilities of the University. Following registration, a username and password will be allocated. Registration for other services may be requested by application to Computing Services.

All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to another person, except to trusted members of Computing Services staff. Attempts to access or use any username, which is not authorised to the user, are prohibited. No one may use, or attempt to use, computing resources allocated to another person, except when authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold his/her identity or tamper with audit trails. A user should take all reasonable precautions to protect their resources. In particular, passwords used must adhere to accepted good password practice.

3) Investigation and Enforcement

Certain activities on the network and centrally provided systems are routinely logged and/or automatically monitored. These include:

- Usage of workstations

- Access to web pages
- Access to software
- Volume of data transfers
- Quantity of email.

In the majority of cases, the primary purpose of such logging is for fault investigation and capacity planning, anomalies may prompt investigation of possible breaches of the Conditions of Use and the information is available when evidence of possible misuse is needed. You are advised that the Computing Services Department regularly scans the University web cache for obscene material as part of the Policy on Obscene material.

4) Policy on obscene material

- The University does not seek to lay down codes of moral behaviour in this area;
- Using the University's network to send or receive obscene material is a breach by the user of conditions of use and additionally may render the University liable to criminal proceedings as a distributor of such material. The University must therefore University a pro-active policy to deter such misuse of facilities.
- It is important to distinguish different kinds of offence. Leaving child pornography aside, the act of viewing obscene material on the internet is not a criminal offence, though it contravenes the Acceptable Use Policy. Any disciplinary consequences should therefore be proportionate and should follow informal warning, initially from the Head of Computing Services rather than via the Head of Department.
- By contrast, the distribution of obscene material (including the circulation of it to another user) is capable of being a criminal offence and should be dealt with under the disciplinary procedures, which provide for discretion in the matter of report to the Police.

Offences involving child pornography should be reported to the Police in all cases. The Computing Services Department will selectively monitor all incoming internet traffic by occasionally scanning the University web cache for obscene material. The scan will look for internet addresses listed on selected link sites devoted to definitely obscene material. When a user is found to have made use of such an address, his or her internet traffic will be examined in detail to see whether the usage is part of a systematic pattern of misuse. No adverse action will be taken if the misuse is not systematic since it is recognised that occasional calls to sites that prove to contain obscene material can readily be made inadvertently.

5) Privacy

It should be noted that Computing Services staff, who have appropriate privileges, have the ability to access all files, including electronic mail files, stored on a computer which they manage.

Access to staff files will not normally be given to another member of staff unless authorised by the Head of Computing Services, who will use his/her discretion in consultation with a senior officer of the University, if appropriate. In such circumstances the Head of Department or Section, or more senior line manager, will be informed, and will normally be consulted prior to action being taken. Such access will normally only be granted where a breach of the law or this policy is suspected.

Student privacy is seen by the University as a privilege and not a right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff. Systems staff are authorised to release the contents of a student's files to any member of staff who has a work-based reason for requiring this access.

Files, which are left behind after a student or member of staff leaves the University, will be considered to be the property of the University.

6) Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the University's computer systems is jeopardised if users do not take adequate precautions against malicious software, such as

computer virus programs. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Conventional norms of behaviour apply to computer based information technology just as they would apply to more traditional media. Within the University setting this should also be taken to mean that the traditions of academic freedom will always be respected.

Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene University codes on harassment. Users of University computer systems must make themselves familiar with, and comply with, the University codes concerning all forms of harassment.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

For specific services the University may provide more detailed guidelines. Users of services external to the University are expected to abide by any rules and codes of conduct applying to such services.

7) Definitions of Acceptable & Unacceptable Usage

Unacceptable use of University computers and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under Cyprus and international law; propagation will normally be considered to be a much more serious offence;
- causing annoyance, inconvenience or needless anxiety to others;
- defamation (genuine scholarly criticism is permitted);
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
- unsolicited advertising, often referred to as "spamming";
- attempts to break into or damage computer systems or data held thereon;
- attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- the distribution or storage by any means of pirated software,
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs, such as the use of peer-to-peer file sharing applications,
- frivolous use of University owned Computer laboratories, especially where such activities interfere with others' legitimate use of IT services,
- the deliberate viewing and/or printing of pornographic images and videos,
- the passing on of electronic chain mail,
- the use of departmental academic mailing lists for non-academic purposes,
- the purchase of blank CDs for the purpose of copying unlicensed copyright software or audio CDs,
- the use of other people's web site material without the express permission of the copyright holder.

Other uses may be unacceptable in certain circumstances. In particular, users who bring their own personal computers e.g. laptops, should take account of the particular conditions of use applying to that service. It should be noted that laptop users should not provide any services to others via remote access. The installed machine on each network socket must be a workstation only and not provide any server-based services, including, but not limited to, Web, FTP, IRC, Streaming Media or e-mail services.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via electronic mail that they have read, but have never viewed.

Acceptable uses may include: personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others; and advertising via electronic notice boards, intended for this purpose, or via other University approved mechanisms. However such use must be regarded as a privilege and not as a right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

Users are strictly prohibited from connecting/installing personal wireless access points and/or other network/routing equipment on the University network. All such rogue equipment can and do interfere with the normal operation of the network and as such their usage is strictly prohibited without prior written consent from the Computing Services Department.

8) Legal Constraints

Any software and/or hard copy of data or information which is not generated by the user personally and which may become available through the use of University computing or communications resources shall not be copied or used without permission of the University or the copyright owner. In particular, it is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software and/or information provided by the University may only be used as part of the user's duties as an employee or student of the University or for educational purposes. The user agrees to abide by all the licensing agreements for software entered into by the University with other parties.

In the case of private work and other personal use of computing facilities, the University will not accept any liability for loss, damage, injury or expense that may result.

9) University Discipline

Staff or students who break this Acceptable Use Policy will find themselves subject to the University's disciplinary procedures and may be subject to criminal proceedings. The University reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

10) Policy Supervision and Advice

The responsibility for the supervision of this Acceptable Use Policy is delegated to Computing Services.

Any suspected breach of this policy should be reported to a member of Computing Services staff. The responsible senior member will then take the appropriate action within the University's disciplinary framework, in conjunction with other relevant branches of the University. Computing Services staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. The University reserves the right to audit and/or suspend without notice any account pending any enquiry.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses which are not fully covered. In the first instance students should address questions concerning what is acceptable to their supervisor; staff should initially contact their departmental I.T. Acceptable Use Policy Adviser or Head of Department/Section. Where there is any doubt the matter should be raised with Computing Services, whose staff will ensure that all such questions are dealt with at the appropriate level within the University.