Acceptable User Policy

Introduction

The University of Kelaniya seeks to promote and facilitate the proper and extensive use of Information Technology (IT) in the interests of learning, working and research. Whilst the tradition of academic freedom will be fully respected, this also requires responsible, ethical and legal use of the technologies and facilities made available to students and staff of the University.

The Acceptable Use Policy is intended to provide a framework for such use of the University's IT resources. It applies to all computing, telecommunication, and networking facilities provided by the ICT Centre, any faculty, department or section of the University.

1. Purpose of Use

1.1 University IT resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the University. No use of any IT service should interfere with another person's duties or studies or any other person's use of IT systems, nor bring the University into disrepute, in any way

1.2 Priority of using University-owned facilities must always be granted to those needing facilities for academic or other essential work. Uses for non-work-related purposes, such as personal electronic mail or recreational use of the World Wide Web including social networking sites, are understood to enhance the overall experience of an employee or student but are not an absolute right

1.3 University e-mail addresses and associated University e-mail systems must be used for all official University activities. All staff and students of the University must regularly read their University e-mail

1.4 Use of IT facilities for commercial work for outside bodies, requires explicit permission from the relevant authorities

2 User Authorization

2.1 In order to use the computing facilities of the University a person must first be registered. Registration of all members of staff and registered students is carried out automatically. Others must apply to IT Services. Registration to use University services implies, and is conditional upon, acceptance of this Acceptable Use Policy

2.2 The registration procedure grants authorization to use the core IT facilities of the University. Following registration, a username, password and an e-mail address will be allocated. Authorization for other services may be provided by respective faculties, departments, centres, units, administrative branches, etc.

2.3 All individually allocated items such as usernames, passwords and e-mail addresses 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 any other person, other than to designated members of IT staff for the purposes of system support. Users should never provide their username and password through an email or over the telephone

2.4 Attempts to access or use any username, e-mail address or certificate, which is not authorized to the user is prohibited. No one may use, or attempt to use, ICT resources allocated to another person, except when explicitly authorized by the provider of those resources under exceptional circumstances

2.5 All users must correctly identify themselves at all times. A user must not impersonate another, withhold their identity or tamper with audit trails

2.6 A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice. Advice on what constitutes a good password may be obtained from ICT Centre Web pages. This advice must be followed: failure to do so may be regarded as a breach of this policy

3 Privacy of Users

3.1 It should be noted that systems staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on any computer which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of users

3.2 The University fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit. Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services,
- prevent a breach of the law, this policy, or other University policy,
- investigate a suspected breach of the law, this policy, or other University policy,
- monitor standards.

3.3 Access to staff files, including electronic mail files, will not normally be given to another member of staff unless explicitly authorized by a Dean of the Faculty, Head of the Department, Head of the Centre or Unit, or Officer in charge. Such access will normally only be granted in the following circumstances:

- where the staff requires access to e-mail messages or files of an individual, which are records of a university activity, and the individual is unable (e.g. through absence) to provide them,
- where a breach of the law or a serious breach of this or another University policy is suspected,
- when a documented and lawful request from a law enforcement agency has been received.

3.4 The University sees student privacy as desirable but not as an absolute right. Systems staff are authorized to release the contents of a student's files, including electronic mail files under following circumstances:

- when a breach of the law or of this policy is suspected,
- when a documented and lawful request from a law enforcement agency has been received,
- when required by any member of staff who has a direct academic work-based reason.

3.5 After a student or member of staff leaves the University, files which are left behind on any computer system owned by the University, including servers, and including electronic mail files, will be considered to be the property of the University

3.6 When leaving the University, staff should make arrangements to transfer to colleagues any e-mail or other computer-based information held under their personal account where appropriate, as access authorizations are terminated within 60 days of their departure

4 General Conditions

4.1 No person shall jeopardize the integrity, performance or reliability of computer equipment, software, data and other stored information

4.2 The integrity of the University's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer virus programs

4.3 All users of the University’s IT services must ensure that any computer for which they have responsibility, and which is attached to the University network, is adequately protected against viruses, through the use of up to date anti-virus software and has the latest tested security patches installed

4.4 Reasonable care should also be taken to ensure that resource use does not result in a denial of service or drop in quality of service to others

4.5 Conventional norms of behaviour apply to IT-based media, just as they would apply to more traditional media

4.6 Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene the University’s accepted codes of practice

4.6 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 unauthorized 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

4.7 It should be noted that individuals may be held responsible for the retention of attachment material that they have received via e-mail that they have read. Similarly, opening an attachment received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in individual users being held responsible

4.8 Those buying IT equipment must adhere to the University's current purchasing policies relating to such purchases. This applies particularly to the purchase of laptop and desktop computers, for which there is a specific policy in place

4.9 Users of services external to the University are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and will be dealt with accordingly. This includes electronic databases, social networking sites, blog and wiki services, bookmarking services and any other external services, including those described as Web 2.0 or otherwise.

4.10 The use of the University’s credentials to gain unauthorized access to the facilities of any other organization is prohibited

4.11 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 must abide by all the licensing agreements for software entered into by the University with other parties, noting that the right to use any such software outside the University will cease when an individual leaves the institution

4.12 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

5 Acceptable & Unacceptable Usage

5.1 Acceptable uses may include:

- use of ICT resources for teaching, learning, research, administration or any other official activities of the University
- 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
- advertising via electronic notice boards/forums, intended for this purpose, or via other University approved mechanisms
- However such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

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

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognized research or teaching that is permitted under university regulations and common law; propagation will normally be considered to be a much more serious offence
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights, including use internal to the University, e.g. on Learn
- causing annoyance, inconvenience or needless anxiety to others
- defamation (genuine scholarly criticism is permitted)
- unsolicited advertising, often referred to as "spamming"
- sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address
- attempts to break into or damage computer systems or data held thereon
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software
- attempts to access or actions intended to facilitate access to computers for which the individual is not authorized
- using the University network for unauthenticated access
- attempts to disrupt services of IT systems including e mail, web based and other related services

5.3 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 downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid license, or other valid permission from the copyright holder
- the publication on external websites of unauthorized recordings, e.g. of lectures

- the distribution or storage by any means of pirated software
- connecting an unauthorized device to the University network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, IT purchasing policy, and acceptable use
- circumvention of Network Access Control
- monitoring or interception of network traffic, without permission
- probing for the security weaknesses of systems by methods such as port-scanning, without permission
- associating any device to network Access Points, including wireless, for which you are not authorized
- non-work and non-study related activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs
- excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action
- use of University owned computer laboratories unnecessarily, especially where such activities interfere with others' legitimate use of IT services
- opening an unsolicited e-mail attachment, especially if not work or study-related;
- the deliberate viewing and/or printing of pornographic images
- the passing on of electronic chain mail causing problems for other users
- posting of defamatory comments about staff or students on social networking sites
- the creation of web based content, portraying official University activities without express permission or responsibility
- the use of University mass mailing lists for non-work purposes
- the use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.
- the copying of other people's Web site, or other, material without the express permission of the copyright holder
- the use of peer-to-peer and related applications within the University. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, etc.
- Plagiarism, i.e. the intentional use of other people's material without attribution

6 Legal Constraints

6.1 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 license for the use of the software or information and to abide by them.

7 University Discipline

7.1 Staff or students who break this Acceptable Use Policy will be subjected to the University's disciplinary procedures. The Vice Chancellor or an official on behalf of the Vice Chancellor may take such disciplinary action. Individuals may also be subject to criminal proceedings

7.2 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

8 Policy Supervision and Advice

8.1 The responsibility for the supervision of this Acceptable Use Policy is delegated to the ICT Centre. Procedural guidelines will be published from time to time as a separate document

8.2 Any suspected breach of this policy should be reported to a member of staff of the ICT Centre. The ICT Centre staff will also take action when infringements are detected in the course of their normal duties

8.3 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. Where necessary, this will include the interception of electronically mediated communications

8.4 This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered