THE UNIVERSITY OF AUCKLAND
NEW ZEALAND
Te Whare Wānanga o Tāmaki Makaurau

NetSafe
The Internet Safety Group

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

VERSION 1.0

This policy document is issued by the Vice-Chancellor's Office.
It is administered through the IT Strategy & Policy Committee.
Compliance is a requirement under the Application for Admission declaration made by all persons seeking admission under the Admission Regulations and is either implied or explicit in University of Auckland employment contracts.

CONTENTS

PART A - INTRODUCTORY INFORMATION

In this document the following definitions apply;

Information and Communications Technology (ICT)

"ICT" means all information and communications technology hardware and software, data and associated methodologies, infrastructure and devices that are:

a) controlled or operated by the University:
b) connected to the University network:
c) used at or for University activities:
d) brought onto a University site.

ICT includes but is not limited to; computers (such as desktops, laptops, PDAs), computer systems, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), telecommunication equipment, networks, databases and any other similar technologies as they come into use.

User

"User" means anyone who operates or interfaces with ICT. It includes University staff, officers and students (whether permanent, temporary or part-time), honorary staff, contractors, sub-contractors, consultants, business partners or official visitors or any other member of the University.

Authorised person

"Authorised Person" means a member of the University staff;

Refer to The University of Auckland Disciplinary Statute 1998 and ICT Statute 2007 for other relevant definitions.

It is a condition of use that all Users abide by the terms and conditions of the ICT Acceptable Use Policy. The use of ICT must always be consistent with the University’s statutory obligation to maintain the highest ethical standards.

All members of the University community benefit from being party to the University’s ICT safety and security programme which endeavours to ensure the safe use of ICT within the University and communities served by the University. The ICT Acceptable Use Policy applies to all Users and ICT at any time.

Under the Admission Regulations (a statute of The University of Auckland) and implied or explicit in University of Auckland employment contracts, Users are required to abide by the statutes and regulations of The University of Auckland (UoA) and to comply with the reasonable requirements of The University of Auckland. You must read this policy document carefully as a reasonable requirement and you are further advised to print off, or make an electronic copy of, this document for later reference.

PART B - ICT SAFETY: general conditions and rules

1. Requirements regarding acceptable use of ICT

1.1. The University provides ICT for its educational purposes, particularly teaching and research, as well as for reasonable personal use which is acceptable to the University environment.

This means that the use of ICT must not be illegal and must be of the highest ethical standards (see S161, Education Act 1989). Further it means that ICT use must not include involvement with material unacceptable to the University environment, acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT without authorisation, plagiarism, gaming, impersonation/identity theft, spoofing, gambling, or cheating in an examination. Behaviour the University may need to respond to also includes the use of websites to facilitate misconduct. Any exception under this policy to permit course content or work involving material which, in other circumstances could be deemed unacceptable to the University environment, must be held in writing and signed by a Head of Department.

Illegal as used in this clause could include involvement with material defined as “objectionable” in the Films, Videos and Publications Classification Act 1993 such as material describing or depicting child sexual abuse, extreme violence or extreme cruelty; or involves communicating material that is knowingly deceptive or misleading; or involvement with an activity such as fraud, defamation, or copyright breach.

1.2. The use of ICT brought onto the University site, or to any University-related activity, must be acceptable to the University environment as detailed in 1.1. For example, **this includes the use of mobile phones and digital cameras** and the display of any images or material present or stored on ICT.

Any User unsure about whether or not it is acceptable to have a particular device at the University or at a University-related activity, or whether the planned use of a particular device meets policy requirements, must check with an Authorised Person responsible for the activity. Note that examples of a *University-related activity* include, but are not limited to, a field trip, camp, sporting or cultural event, *wherever its location*.

1.3. Users are responsible for any use of their computer account; for example if an individual user name is shared or the password divulged, the holder of the account may be held personally responsible for any actions that arise from the misuse of the account.

1.4. Those provided with individual, class or group email accounts are expected to use them in a responsible manner and in accordance with the requirements of this policy. This includes ensuring that no electronic communication made by a User is likely to cause offence to others or harass or harm them, put the owner of the user account at potential risk, or in any other way breach the requirements of 1.1. The Email Usage Policy contains further information.

2. Responsibilities regarding access to unacceptable or illegal material (see B 1.1)

2.1. When using ICT on a UoA site or in connection with any University-related activity, it is a breach of policy to:

- access or initiate access to material that is illegal or unacceptable to the University environment
- save or distribute such material by downloading, copying, storing or printing

If you accidentally access illegal, or what appears to be illegal, material a copy may remain on your computer. A later routine audit could find this copy. To protect yourself in the case of accidental access these steps must be followed;

1. The material must not be shown to others and the display window should be closed immediately
2. The incident should be immediately reported to the IT Service Desk (x 85100) who will log the incident
3. The incident should be reported as soon as is practicable to an Authorised Person

3. Confidentiality and privacy.

3.1. The principles of confidentiality and privacy extend to accessing or inadvertently viewing information about staff or students which is stored on the University network or any device. Users must not seek out or use any such information unless they have been granted specific authority to do so (See B 1.1.) Users need to respect confidentiality and report any matter of concern to an Authorised Person.

4. Disclosure of personal details

4.1. Users should be very careful when revealing personal information about themselves or others, including home or email addresses, or any phone numbers including mobile numbers.

PART C - ICT SECURITY MEASURES

1. User accounts and passwords

1.1 **Individual user name and password.** Access to University ICT, and Internet access using University ICT, is permitted only through use of an authorised computer account.

1.2 **Confidentiality of passwords**. Users are responsible for keeping their password confidential. Users must not attempt to discover or change any other person's password.

1.3 **Group accounts.** The password of a group account must not be passed on to anyone outside the group. There is a collective responsibility not to alter or delete data accessed using a group account unless authorised.

1.4 **Workplace security.** Users are responsible for either logging-off or securing their computer screen with a password protected screensaver when leaving it unattended.

1.5 **Strength of passwords.** Where systems currently permit it, Users must select a password that conforms to the following University minimum standard

Section 1: Individual passwords

(a) Use a minimum of eight characters and at least one character from three of the following four classes;

- English upper case letters
- English lower case letters
- Numerals (0,1,2,...)
- Non-alphanumeric (special) characters such as punctuation symbols.

(b) Do not base passwords on any easily identified words, numbers, or special characters e.g. commonly used words, reversal of such words, any system identifier or obvious phrases or sequences.

(c) Do not reuse a password; construct a new password each time it is changed.

(d) The following strategies will help you to generate a password that is easy to remember, is hard to guess and complies with the University policy.

- Use a mixture of upper and lower case and punctuation e.g. **kEEpØut!**

- String several words or parts of words together e.g. **it'sCØld**

- Choose a phrase, perhaps a line from a poem or song and form passwords by concatenating words from the phrase along with digits and/or punctuation. e.g. **Tw1nLit*** (from twinkle, twinkle, little star), **yAt55Øm1** (from you are the sunshine of my love)
- Invent phrases like car registration plates e.g. **oNe4yØu!**

Section 2: Group Account passwords

The requirements regarding password complexity apply to Group Accounts. In addition Group Accounts are only permitted if there is a demonstrable need to provide "group" access and in all cases the designated account "owner" remains responsible for their correct use at all times.

NB For further information on effective password creation and account management, see http://www.auckland.ac.nz/security/AccountAndPasswordManagementPolicy.htm

1.6 **Password changes.** Users should change their password if they have any cause to believe it has been compromised in any way and, in any case, at least once a year.

2. Care of UoA ICT

2.1 All UoA ICT should be cared for in a responsible manner. All food, drink, chewing gum etc. must be kept away from UoA ICT.

2.2 Any damage, loss or theft of UoA ICT must be reported immediately to an Authorised Person.

2.3 Users must not cause UoA ICT to become unusable or inaccessible to other Users through abuse or misuse.

2.4 Users must not remove material (e.g. files, printouts) belonging to other Users and must leave all support materials provided by the University (e.g. manuals, removable media, etc.) in the facility.

2.5 Users must not attempt to modify UoA ICT without specific written authorisation.

2.6 Users must not jeopardise the security of any UoA ICT.

2.7 Users must access or use only UoA ICT and data that have been made available for general access, or those which they have been specifically authorised to access.

2.8 Users are expected to practise sensible use to limit wastage of UoA ICT resources or bandwidth. This includes avoiding unnecessary printing, and unnecessary Internet access, uploads or downloads using UoA ICT.

3. Connecting software/hardware

3.1 Unless specifically authorised (see 3.2), or in a setting where public access is expected (see 3.3), Users must not attempt to download, install or connect any unauthorised software or hardware to UoA ICT, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies which may be developed.

3.2 When authorisation has been given by a User's supervisor to connect or install privately-owned ICT, it is on the condition that the University may scan this ICT during the period associated with the authorisation as part of a regular or targeted security check.

3.3 The University provides facilities for Users to connect their own ICT to the University's network. These may be of the form of a wireless network or wired networking in designated facilities. If a User is considering linking any privately-owned ICT to the network, it is on the condition that the following criteria are met:

a) connection is via authorised and approved facilities e.g. to the Electronic Campus (EC) domain via the wireless network
b) access is authenticated by the UoA
c) the machine is patched for all critical security vulnerabilities and is running up-to-date anti-virus and anti-spyware software.

Users can connect privately-owned USB pen drives and storage media to UoA ICT however it is the User's responsibility to ensure that confidential and sensitive information is protected. If the storage medium does not support encryption, then Users must encrypt information prior to copying.

4. Installation of network or system monitoring software

4.1 Users must not intentionally develop or use programs that infiltrate ICT, or damage or alter the software components of ICT, unless carried out in a controlled environment as part of an authorised and sanctioned project or course of study.

5. Copyright and licensing

5.1 Copyright laws and licensing agreements must be observed. Activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products are prohibited. See B 1.1, the brochure *The University of Auckland - Use of copyright materials 2005* and the Academic Honesty and Plagiarism page for further information.

6. Websites

6.1 Users must not set up any web presence which purports to be, or might be reasonably perceived as, an official University of Auckland website, without appropriate authorisation.

7 Monitoring by the University

7.1 The University may monitor, access, and review all use of UoA ICT. From time to time this information may be examined and analysed to help improve the safety and security of UoA ICT. This includes personal emails sent or received using UoA ICT. The University does not routinely inspect or monitor email but does reserve the right to do so under the prescribed conditions defined in the Email Usage Policy. Whilst the University may monitor UoA ICT it does not filter or screen material in order to prevent access.

8 Audits of UoA ICT

8.1 The University as part of its legal requirements and business processes may conduct internal audits of UoA ICT, or may be required to submit to an independent audit. If deemed necessary, auditing will include any stored content, and all aspects of its use, including email. An audit may also include any ICT provided or subsidised by or through the University or related or affiliated organisations.

9 Queries or concerns about technical or security matters

9.1 Users should raise any queries or concerns regarding technical or security matters with the University Information Security Officer (security@auckland.ac.nz).

PART D – Breaches of the ICT Acceptable Use Policy

1. A breach of the ICT Acceptable Use Policy constitutes a breach of the Disciplinary Statute 1998.
2. A breach which is harmful to the safety of a User, or poses a significant threat to the University, may be referred to a law enforcement agency.
3. A breach of this ICT Acceptable Use Policy will otherwise be dealt with:
    a. in the case of a student, under the provisions of University Statutes and Regulations.

    b. in the case of a member of staff, according to the provisions of employment law and the relevant employment agreement.

    c. in the case of a contractor engaged by the University to undertake specified tasks, in accordance with the provisions of the relevant contract.

    d. in the case of a User who may fall into more than one of the above categories by a process determined by the Vice-Chancellor, or the nominee of the Vice-Chancellor, and which takes into account the circumstances of the particular breach.
4. Where a breach of the ICT Acceptable Use Policy is established, but not referred to a law enforcement agency, one or more of the following penalties may be imposed on a person responsible for, or involved in the breach:
    - warning
    - formal written warning
    - restriction or termination of access to UoA ICT, the summary suspension of such access and/or rights pending further actions, including disciplinary action
    - the requirement to provide compensation for any improper use of, or damage to, UoA ICT
    - disciplinary sanctions, which may include dismissal of an employee, termination of a contract or the suspension or expulsion of a student from a course of study
5. A student subject to a penalty may appeal the penalty or the decision or both as set out in the provisions of Clause 11 of the Disciplinary Statute. Such an appeal must be made in writing to the Registrar within 14 days of the penalty having been imposed. The appeal will be heard by the Council’s Appeals Committee.
6. The University views misuse of ICT as a serious matter and may restrict access to its facilities as a result. Students are advised that if alternative facilities are unavailable or not feasible, it may not be possible for them to complete requirements for course work.
7. In the course of investigating a suspected breach of this policy, the University may request permission to audit privately-owned equipment/device(s) where, on reasonable grounds, the University believes such equipment/devices were involved in the alleged incident.
8. Involvement with material deemed ‘objectionable’ (illegal), under the Films, Videos and Publications Classification Act 1993, or any involvement in an activity which might constitute criminal misconduct, is a very serious matter which may necessitate the involvement of law enforcement in addition to any disciplinary response made by the University as a result of its investigation. The University may be obliged to report such activities to the relevant authorities.