Policy Document

POLICY ON THE USE OF UNIVERSITY INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCES (ICT RESOURCES)

For the definitions of terms used in this policy document refer to the Delegations of Authority. Senior Delegated Officer (SDO) means the manager with the delegated authority for the management of a number of organisational units and/or University wide function(s), ie the relevant DVC or PVC (College). As appropriate for the local nomenclature and reporting lines, when this document refers to Department read also School or Unit; to Faculty read also: Sydney College of the Arts, Sydney Conservatorium of Music or Administrative Unit; to Head read Head of Department/School/Unit; and to Dean read also Director or College Principal. For Head, Dean and PVC read also HOA, Senior Manager and DVC, as appropriate

1 Policy

All Users will be lawful, efficient, economical and ethical in their use of the University's ICT Resources, which are provided to create, preserve, transmit and apply knowledge through teaching, research, creative works and other forms of scholarship.

2 Definitions

ICT Resources
All of the University's Information and Communication Technology Resources and facilities including, but not limited to: mail, telephones, mobile phones, voice mail, SMS, facsimile machines, email, USydNet, MyUni, UniKey, eStaff, the intranet, e-Services, securID, computers, printers, scanners, access labs or other facilities that the University owns, leases or uses under Licence or by agreement, any off campus computers and associated peripherals and equipment provided for the purpose of University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks.

User/s
All employees, including casual employees, any person enrolled in an award course of study at the University and any person registered to attend short courses, seminars or workshops in any unit of the University, including the Centre for English Teaching and the Centre for Continuing Education as well as all other persons including members of the general public, who have been granted access to, and use of, the University's ICT Resources.

A member of the public reading public University web pages from outside the University is not by virtue of that activity alone considered to be a User.

3 Principles

(1) The University's ICT Resources exist and are maintained to support the work of the organisation. The University reserves the right to monitor the use of its ICT Resources and to deal appropriately with Users who use its ICT Resources in ways contrary to the conditions of use set out in this policy.

(2) Materials produced using the University's ICT Resources are to be generated subject to the relevant University policies (e.g. privacy and recordkeeping).

(3) The University will exercise its rights with regard to web based and other electronic documents in accordance with its Intellectual Property Rule 2002 (as amended).

(4) The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources.

4 Coverage

This policy document applies to all Users of the University's ICT Resources.

5 Conditions of Use

Use of the University's ICT Resources is restricted to legitimate University purposes only.

For students this generally means academic coursework and research as approved by a supervisor. Staff usage will depend on the nature of their work.

The use of University ICT Resources through non-University (including personally owned) equipment is also subject to this policy.

To assist Users to understand the implications of the above condition the following examples of prohibited and permitted use are provided. These examples are indicative only.

a) The University will not tolerate its ICT Resources being used in a manner that is harassing, discriminatory, abusive, rude, insulting, threatening, obscene or otherwise inappropriate.

   It is illegal to use any ICT Resource to harass, menace, defame, libel, vilify, or discriminate against any other person within or beyond the University. It is important to understand that in matters of discrimination and harassment it is the **reasonable perception of the recipient** and not the intention of the sender that is significant.

   Users may be individually liable if they aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. Users who adversely affect the reputation of another person may be sued for defamation by that aggrieved person.

b) Users must not use the University's ICT Resources to collect, use or disclose personal information in ways that breach the University's Privacy Policy.

c) Users must respect and protect the privacy of others.

d) Users are forbidden to use ICT Resources to access, store or transmit pornographic material of any sort other than with specific written approval from an authorised University Officer for research related purposes.

e) The use of ICT Resources for gambling purposes is forbidden.

f) The University forbids the use of its ICT resources in a manner that constitutes an infringement of copyright. The law permits copying and/or printing only with the permission of the copyright owner, with a few very limited exceptions such as fair use for study or research purposes (this exception itself is subject to numerous provisos and conditions in the Copyright Act).

   Accordingly Users must not download and/or store copyright material, post copyright material to University websites, transfer copyright material to others or burn copyright material to CD ROMs or other storage devices using ICT Resources, **unless the copyright material is appropriately licensed.**

   Copyright material includes software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s) and video files.

g) ICT Resources must not be used to cause embarrassment or loss of reputation to the University.

h) The University does not permit the use of its ICT Resources for unauthorised profit making or commercial activities. Academic staff are referred to the University's Outside Earnings Policy with regard to the use of University Resources for private professional practice. General staff are referred to the University's Code of Conduct.

i) All internet content made available on the University's ICT Resources must comply with the University's policy on Internet Content.

j) Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the network. They may only delete and alter data as required by their authorised University activities

   Note: This does not apply to specially authorised University computing staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.

k) Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorised and competent to do so. All faults or suspected faults must be reported to either the relevant departmental computer services officer or IT Services Helpdesk.

l) ICT Resources must not be used to distribute unsolicited advertising material from organisations having no connection with the University or involvement in its activities.

m) Users of University issued accounts must identify themselves and not use a false identity.

n) University email lists generated for formal University communications must not be used for other than University business.
o) Unless via a personally paid account, files may only be accessed or downloaded if they are work or study related. In any case, files may only be downloaded if it is legal to do so and steps have been taken to ensure that the files are free from viruses and other destructive codes.

p) Files may only be attached to email messages if the sender believes they are free from viruses and has taken steps to ensure that they do not contain viruses or other destructive code.

q) Users must not attempt to gain unauthorised access to any computer service. The use of another person's login, password or any other security device (e.g. SecurID, digital signature or biometric identification) is not permitted. Nor must Users exploit any vulnerabilities in systems or (except authorised staff when checking security of systems as part of their duties) use any technology designed to locate such vulnerabilities or circumvent security systems. Such behaviour is likely to be a breach of Part 6 of the NSW Crimes Act 1900 and if proven would potentially be considered serious misconduct and accordingly may be dealt with under relevant disciplinary provisions. The matter may also be referred to the police and/or the Independent Commission Against Corruption.

r) Users must not use ICT Resources for the purposes of subscribing to and accessing fee based services that are for personal use only, unless the subscription or access is from a personally paid account and the Users personally pay the fees for the services and the services are legal.

s) Users must not facilitate or permit the use of the University's ICT Resources by persons not authorised by the University e.g. Users must not set up a wireless relay base station from their University accounts.

t) Limited minor and incidental personal use may be allowed, but it is a privilege and must not interfere with the operation of ICT resources, burden the University with incremental costs, interfere with the User's employment or other obligations to the University and is subject to compliance with University policies. Users should be aware that personal use of the University's ICT Resources may result in the University holding personal information about the User and/or others which may then be accessed and used by the University to ensure compliance with this, and other policies.

6 Monitoring

(a) Use of ICT Resources is not considered private. Users of ICT Resources should be aware that they do not have the same rights as they would using personally owned equipment through commercial service providers.

(b) The University's electronic communication systems generate detailed logs of all transactions and use. All Users should be aware that the University has the ability to access these records and any backups. In addition, system administrators have the ability to access the content of electronic communications and files sent and stored using the University's equipment.

(c) The University charges telephone calls and Internet charges back to schools/departments. This means that managers are regularly advised of postal expenditure, the costs of all telephone calls from each extension and Internet traffic costs associated with each network connection/computer. Users should be aware that details of telephone numbers called are recorded and can be accessed.

(d) The University reserves the right to audit regularly and monitor the use of its ICT Resources to ensure compliance with this policy.

(e) The University also reserves the right to look at and copy any information, data or files (including non-University material) created, sent or received by Users using, or while connected to, the University's ICT Resources in the event of a suspected breach of this or other policies.

7 Response to Breaches

(a) The University reserves the right to withdraw, restrict or limit any User's access to its ICT Resources if a breach of these conditions is suspected. Any such suspected breach may also be investigated under other University processes, and may result in disciplinary action being taken against the offender in accordance with those processes. This may include a request to reimburse costs (e.g. for unreasonable personal use), disciplinary action (including termination of employment/suspension of candidature) and /or criminal prosecution.

(b) Further the University reserves the right to remove or restrict access to any material within the University domain. Such decisions will be communicated to the appropriate supervisor and account holder.

8 Security, Confidentiality and Privacy

(a) Matters of a confidential nature should only be conveyed or stored in an electronic format when adequate security measures have been taken.

(b) While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection confidentiality, privacy or security of any information.

(c) Email and other records stored in ICT Resources may be the subject of a subpoena, search warrant, discovery order or application under the NSW Freedom of Information Act 1989. Disclosure outside the University of any personal information, irrespective of its format, will be in accordance with the NSW Privacy and Personal Information Protection Act 1998, the Health Records and Information Protection Act 2002, the University's Privacy Policy and its *Privacy Management Plan*.

(d) While the NSW Privacy and Personal Information Protection Act, and the NSW Health Records and Information Protection Act 2002 and the expression of these in the University Privacy Policy, regulate the collection, management, use, security and disclosure of personal information, the Act and the Policy do not confer an automatic right of privacy for Users accessing ICT Resources. The University may collect and receive personal information of Users and others in the course of managing the operation and use of its ICT Resources and that information can be used in connection with efforts to ensure that Users comply with all relevant laws and University policies.

(e) Communications on University business in any format or media are official records, subject to statutory record keeping requirements and the University Recordkeeping Policy. This includes email sent and received by staff members on any University related matter. Staff need to be conscious of the need to preserve official communications in accordance with the relevant University guidelines on the management of electronic records. Care should be taken before

deleting any electronic communication that it is not required to be kept as evidence of a decision, authorisation or action.

(f) Sending an email on an official University matter is similar to sending a letter on University letterhead. Such email transactions should be handled with the normal courtesy, discretion and formality of all other University communications. Users should **not** write anything in an email that they would not sign off in a memorandum.

9 Background/Context

This policy replaces the USydNet Conditions of Use and sets out the standards of acceptable, legal and ethical use expected of Users of University ICT Resources. In addition, it sets out the circumstances in which monitoring of use of communication Resources will occur and addresses the associated issues of privacy and recordkeeping.

10 Authority/consultation

This policy has been developed by the Acting Chief Information Officer in consultation with the Information Technology Portfolio Services, Solicitor's Office, Registrar, Chair of the Academic Board, Archives and Record Management Services, FOI Co-ordinator and Personnel Services.

Management responsibility

Senior Deputy Vice-Chancellor

Implementation responsibility
Academic and Administrative Heads.

11 Approval

By

_____
Senior Deputy Vice-Chancellor

Date_____

Date of Effect
Date_____

Proposed Date of Review
12 months from date of approval

12 References

(1) Legislation and other external sources

Anti-Discrimination Act 1977
Broadcasting Services Amendment (Online Services) Act 1999 (Cth)
Copyright Act, 1968 (Cth)
Crimes Act, 1914 (Cth)
Crimes Act, 1900
Disability Discrimination Act 1992 (Cth)
Freedom of Information Act 1989
Health Records and Information Privacy Act 2002
Human Rights and Equal Opportunity Commission Act 1986 (Cth)
Independent Commission Against Corruption Act 1988
Privacy and Personal Information Protection Act 1998
Racial Discrimination Act 1975 (Cth)
Sex Discrimination Act 1984 (Cth)
State Records Act 1998
Telecommunications (Interception) Act 1979 (Cth)
Workplace Relations Act 1996 (Cth)
National Classification Code

(2) University Policies and Guidelines

Academic Board Resolutions: Academic Honesty in Coursework:
Code of Conduct – Staff and Affiliates
Student Code of Conduct
Corruption Prevention Strategy:
University of Sydney (Delegations of Authority – Administrative Functions) Rule 2010 (as amended)
Freedom of Information Policy
Harassment and Discrimination Prevention Policy and Resolution Procedure
University of Sydney (Intellectual Property) Rule 2002
Outside Earnings of Academic Staff Policy and Procedures 2011
University Privacy Policy
University of Sydney Privacy Management Plan
http://sydney.edu.au/arms/privacy/pmp.pdf
University Recordkeeping Policy
Reporting Corruption, Maladministration or Serious and Substantial Waste of Public Money
University of Sydney Enterprise Agreement 2009 – 2012