



Information Technology Services

EMAIL ACCESS POLICY

Date approved:	13 April 2004	Date Policy will take effect:	13 April 2004	Date of Next Review:	
Approved by:	Vice Chancellor				
Custodian title & e-mail address:	Senior Manager Business Services Uni michele_grange@uow.edu.au				
Author:	Michele Grange				
Responsible Faculty/ Division & Unit:	Business Services Unit, Information Technology Services Division				
Supporting documents, procedures & forms of this policy:	Nil				
References & Legislation:	Crimes Act, 1914 (Commonwealth) State Records Act, 1998 (NSW) IT Acceptable Use Policy (including the Requirements Governing the Use of IT Facilities) Student Conduct Rules				
Audience:	Public – accessible to anyone				
Expiry Date of Policy:	Not applicable				



Contents

[1 Purpose of Policy.....3](#)

[2 Definitions.....3](#)

[3 Application & Scope.....3](#)

[4 Acceptable Use3](#)

[5 Email Quota System.....3](#)

[6 Ownership.....3](#)

[7 Confidentiality.....4](#)

[8 Authentication and Integrity.....4](#)

[9 Unsolicited Mail.....4](#)

[10 Administration and Implementation.....5](#)

[11 Roles & Responsibilities.....5](#)

[12 Version Control and Change History.....5](#)



1 Purpose of Policy

1. This policy outlines the University's provision of email to the University community.
2. The University of Wollongong is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative and service functions. This policy is an adjunct to the University's IT Acceptable Use Policy, which defines the acceptable behaviour expected of users and intending users of the facilities, including email. The University requires users to accept the IT policies and the associated Requirements Governing the Use of IT Facilities as a condition of their use. These are accessible on the University Policy Directory.

2 Definitions

Word/Term	Definition (with examples if required)
Email	Electronic mail messages
University	University of Wollongong
User	Any person using any of the University's Information Technology Facilities
IT facilities	Information Technology facilities operated by the University, whether owned or leased
Chief Technology Officer	The Chief Technology Officer, Information Technology Services
ITS	Information Technology Services at the University of Wollongong

3 Application & Scope

1. This policy applies to all usage of the University electronic mail services. This policy represents the University Institutional position and takes precedence over other relevant policies which may be developed at a local level.
2. All users should be aware of the policy, their responsibilities and legal obligations. All users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4 Acceptable Use

1. The University encourages the use of the Internet, including email and web services, to facilitate communication among internal users and with the external community to allow users to better perform the duties assigned to them; and to allow greater efficiency in teaching, research, administrative and service functions.
2. To utilise the University's email it is necessary to have a user account. The University's IT Acceptable Use Policy defines the acceptable behaviour expected of users of the facilities. All users should be aware of their obligations under this policy.

5 Email Quota System

1. The University may apply a quota for email storage on the mail servers. The Chief Technology Officer will review any applied quotas on an ongoing basis.

6 Ownership

1. Email messages sent and received through the email services provided by the University are records of University activities. Thus email messages have the same status as other written communications or records, and are to be treated accordingly.



-
2. Email messages are bound by the provisions of the State Records Act, 1998 (NSW). Information on the act is available at <http://www.records.nsw.gov.au>.

7 Confidentiality

1. Whilst the University seeks to preserve privacy and confidentiality in the provision of all IT Services, confidentiality of electronic mail cannot be assured. Confidentiality may be compromised by unintended redistribution, or due to technologies which may not protect against unauthorised access. In addition, any confidentiality may be subordinate to the application of law or policy, including this policy.
2. Users should assume that the contents of email may be accessible to persons other than the recipient.
3. Users should be aware that, during the performance of their duties, network and systems administrators need to observe the contents of certain data, on storage devices and in transit, to ensure proper functioning of the University's IT facilities. During these processes the contents of email messages may be visible.
4. The University has a legitimate right to capture and inspect any data stored or transmitted on the University's IT facilities (regardless of data ownership), when investigating system problems or potential security violations, and to prevent, detect or minimise unacceptable behaviour on that facility. This includes where maintaining system security and integrity including the management of unsolicited mail and virus protection.
5. The contents of electronic mail will not be released to persons within or outside of the University, except in response to:
 - a. permission from the user; or
 - b. a request from the Senior Executive, Dean, Director or University Librarian, made in writing and accepted by the Chief Technology Officer or delegated persons, to investigate a potential breach of policy; or
 - c. a request from the Senior Executive, Dean, Director or University Librarian, made in writing and accepted by the Chief Technology Officer or delegated persons, for access to be granted; or
 - d. where deemed appropriate by the University in order to uphold the statutory rights of individuals in matters such as privacy, copyright, occupational health and safety, equal employment opportunity, harassment and discrimination; or
 - e. a proper request from an appropriate law-enforcement officer investigating an apparently illegal act, including a court order; or
 - f. a relevant statute.
6. Access to any data will always be via network or systems administrators, or via persons nominated by the Chief Technology Officer. The University's policy and statutory legislation relating to privacy will be upheld in all cases.

8 Authentication and Integrity

1. The University cannot guarantee the authentication or integrity of an email with current technology. That is, it cannot guarantee that the apparent sender is indeed the sender or that the delivered contents are as created by the sender.

9 Unsolicited Mail

1. The University reserves the right to instigate measures to reduce the prevalence of unwanted or unsolicited email (SPAM). This may include blocking mail from known SPAM friendly sites, the moderation of email lists and recommendations for email client configurations.



10 Administration and Implementation

Compliance

1. The University treats misuse of its IT facilities seriously. Violations of the conditions of use of IT facilities may result in temporary or indefinite withdrawal of access, disciplinary action under the University's, or relevant entities, discipline procedures, and/or reimbursement to the University.
2. IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Technology Officer or their nominee will be the Primary Investigation Officer of allegations of IT misconduct by students. Detailed investigation procedures and the penalties that may be awarded to students engaging in IT misconduct can be found in the Student Conduct Rules.
3. A user's access will be withdrawn given a written request from an appropriate staff member of the sponsoring organisation. Access may also be withdrawn by ITS in response to a suspected policy violation.
4. A student whose IT access has been withdrawn as a result of an investigation under the Student Conduct Rules can appeal the decision or the penalty to the Student Conduct Committee. Otherwise, a user whose access has been withdrawn may request reconsideration of the decision by the Chief Technology Officer who shall consider the withdrawal with the relevant Senior Executive, Dean or Director or the University Librarian. Following this the Chief Technology Officer shall confirm the withdrawal or reinstate access.
5. Misuse or unauthorised use of University IT facilities may constitute an offence under the Crimes Act, 1914 (Commonwealth) and/or other pieces of State or Commonwealth legislation. Nothing in this policy or the Requirements Governing the Use of IT Facilities may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.
6. Users are encouraged to report any misuse and any reports will be treated as confidential.

11 Roles & Responsibilities

Not Available.

12 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	13 April 2004	Vice Chancellor	Initial policy
2	1 July 2004		Various changes: Policy converted into new ITS policy format. Included compliance section, consistent with IT Acceptable Use Policy. Improved links to IT Acceptable Use Policy. Removed reference to email etiquette
3	1 September 2004	Vice Chancellor	ITPAC and IT Forum approved version
4	6 May 2009	Vice Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh