



TELEPHONE POLICY

Date approved:	13 March 2004	Date Policy will take effect:	13 March 2004	Date of Next Review:	December 2010
Approved by:	Vice Chancellor				
Custodian title & e-mail address:	Senior Manager, Business Services Unit michele_grange@uow.edu.au				
Author:	Michele Grange				
Responsible Faculty/ Division & Unit:	Business Services Unit, Information Technology Services				
Supporting documents, procedures & forms of this policy:	UOW Telephony Services Web Information				
References & Legislation:	IT Acceptable Use Policy (including the Requirements Governing the Use of IT Facilities) Student Conduct Rules Crimes Act, 1914 (Commonwealth) Mobile Telephone Policy				
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 Telephone Installation and Management3](#)

[5 Acceptable Use.....4](#)

[6 Access to Telephone Accounts.....4](#)

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

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

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



1 Purpose of Policy

1. This document outlines the University of Wollongong policy on telephones and covers telephone installation and management. Mobile Telephones are covered in the Mobile Telephone Policy accessible on the University Policy Directory. Further information on Telecommunications Services at the University of Wollongong is available at <http://www.uow.edu.au/its/telecommunications/index.html>.
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 telephones. The University requires users to accept the IT policies and the 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)
University	University of Wollongong
User	University staff and other authorised users of a University telephone
Telephone	A telephone handset
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 and the associated rules apply to all University telephone 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 as well as 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 Telephone Installation and Management

1. The following apply:
 - 1.1. ITS will be responsible for the installation of telephone cables. Under no circumstances should a third party be allowed to install any telephone cables on the University premises without authorisation from the Chief Technology Officer. This does not apply to cables connecting the wall socket to the telephone handset.
 - 1.2. ITS charge an annual line and socket charge to cover the cost of maintenance and rental which is debited annually from the account nominated by the unit for telephone usage.
 - 1.3. Voice mail is an additional service which is available on request and incurs an additional monthly charge per extension.
 - 1.4. The access of each telephone handset will be classified as follows:
 - University internal access only



- Access to the areas covered by the local telephone exchange only (default)
 - Extensions with national access
 - Extensions with international access
2. Generally international access is limited to the Head of Unit. Call forwarding for each extension can also be limited with access set to internal calls only by default. A request to alter the level of access on any telephone extension must be channelled through the relevant Dean, Director, University Librarian or approved delegate to ITS.
 - 2.1. A User requesting the University call centre to connect a call to national or international numbers will have that call billed to their extension. The call centre may require approval from the relevant Head of Unit.
 - 2.2. ITS will provide call summaries to units which itemise costs per extension.
 - 2.3. ITS will debit telephone usage to the user's unit through a funds transfer process.
 - 2.4. Faults to telephone handsets or lines must be reported to ITS.
 - 2.5. Only telephone handsets supplied by ITS may be connected to the University network. Any damages which occur as a result of connecting a telephone other than those supplied by ITS will be debited to the responsible unit.
 - 2.6. It is advisable that telephone extensions in open access areas, such as a research laboratory, be restricted to internal calls only. PINs (personal identification numbers) for individuals can be organised by contacting ITS.
 - 2.7. ITS will be responsible for the installation and technical support of all public telephones in the University. Under no circumstances will a third party be allowed to install a public telephone on the University premises.
 - 2.8. Depending on the current load on the University's telephone system local calls may fall to a digital line. As a consequence local calls may be charged as a timed local call. Calls should be made on the assumption that this is the case.
 - 2.9. The University does not permit the use of 1900, 1930 or 1500 numbers, except where authorised in writing by the Chief Technology Officer.

5 Acceptable Use

1. A University telephone must not be used for conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any law.
2. Users shall not cause, or attempt to cause, security breaches or disruptions to telephone communications. Examples of security breaches include, but are not limited to, accessing calls of which the customer is not an intended recipient or logging into a server or voicemail account that the user is not expressly authorised to access.
3. Harassment is not permitted, whether through language or frequency of telephone calls.
4. The University's IT Acceptable Use Policy defines the acceptable behaviour expected of users of the facilities, including telephones. All telephone users should be aware of their obligations under this policy.

6 Access to Telephone Accounts

1. The University has the right to capture and inspect any telephone call information made on a University telephone to:
 - a. investigate system problems;
 - b. investigate potential security violations;
 - c. maintain system security and integrity;
 - d. prevent, detect or minimise unacceptable behaviour; and



- e. review expenditure charged to a telephone account.
2. Detailed telephone account information collected in the course of any investigation will not be released to persons within or outside of the University, except in response to:
 - a. permission from the user;
 - 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;
 - 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;
 - 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;
 - e. a proper request from an appropriate law-enforcement officer investigating an apparently illegal act, including a court order; or
 - f. a relevant statute.

7 Administration and Implementation

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 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 unauthorized 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.

8 Roles & Responsibilities

1. Roles and responsibilities are as detailed in this policy.

9 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	13 March 2004	Vice-Chancellor	Initial policy



2	17 March 2005	Vice-Chancellor	ITPAC and IT Forum approved version
3	6 May 2009	Vice-Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh
4	9 March 2010	Vice-Principal (Administration)	Future review date identified in accordance with Standard on Policy