UNIVERSITY
OF WOLLONGONG
AUSTRALIA

TELEPHONE AND MOBILE DEVICE USE POLICY

Date first approved: 9 December 2016	**Date of effect:** 9 December	**Date last amended:** (refer Version Control Table)	**Date of Next Review:** August 2024
First Approved by:	University Council		
Custodian title & e-mail address:	Senior Manager Client Services, IMTS paul_morgan@uow.edu.au		
Author:	Senior Manager Client Services, IMTS		
Responsible Division & Unit:	Information Management & Technology Services		
Supporting documents, procedures & forms of this policy:	Delegations of Authority Policy IT Acceptable Use Policy Privacy Policy Student Conduct Rules Asset Management Policy Purchasing and Procurement Policy Asset Disposal Policy		
Relevant Legislation & External Documents:	*Crimes Act 1914* (Commonwealth) *Criminal Code Act 1995* (Commonwealth) *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Commonwealth)		
Audience:	Public		

Submit your feedback on this policy document using the Policy Feedback Facility.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contents

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Purpose of Policy

1. The purpose of this policy is to outline:
    a. the University's provision of Mobile Device/data and Telephone/Voice Services for internal and external services to ensure users and management have a clear understanding of their responsibilities; and
    b. the procedures to be followed when assessing business needs for the use of Mobile Devices, including mobile telephones, tablets and other Mobile Devices, as well as softphones and internal fixed telephones.
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 comply with the IT policies and associated requirements governing the Use of IT Facilities and Services as a condition of their use. These are accessible on the University Policy Directory.

2 Definitions

Word/Term	Definition
Forced Activation Code (FAC)	A security process to implement call restriction while making a call and to prevent calls from being placed by unauthorized users.
Device User	Authorised users of University owned devices and mobile data services.
IMTS	Information Management & Technology Services at the University of Wollongong
IT Facilities and Services	Information Technology facilities operated by or on behalf of the University. This includes services and systems and associated computing hardware and software used for the communication, processing and storage of information.
Mobile Data Service	Any Mobile Data Service that is provided to University staff and paid for by the University for the purposes of fulfilling individual work requirements.
Mobile Device	Any Mobile Device that is provided to University staff and paid for by the University for the purposes of fulfilling individual work requirements.
Telephone	A fixed telephone handset or softphone.
Telephone/Voice Services	Services related to the provision and support of telecommunications provided to the University via the university Telephone service and a range of carrier services.
University	University of Wollongong and controlled entities.
Usage	All calls, messages, data transfers, and services that are attributable to a Telephone or Mobile Device account.
Voicemail	The service allowing messages to be held or replayed on all services.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

3 Application & Scope

1. This policy applies to all University Telephone/Voice and Mobile Data Services, the usage of all Telephones, Mobile Devices and Mobile Data Services and their associated accounts owned by the University.
2. All Users should be aware of the policy, their responsibilities and legal obligations.
3. All Users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4 Acceptable and Unacceptable Use of Telephones, Mobile Telephones and Devices

1. A University Telephone or Mobile Device must not be used for transmission, retransmission, or storing of any unlawful, obscene, indecent, profane, libellous, offensive, pornographic, threatening, abusive, defamatory, or otherwise objectionable information. Without limitation this includes any transmissions constituting or encouraging conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any law.
2. All users or Data Services must accept full responsibility for using their University Telephone, Mobile Device in an honest, ethical, safe and legal manner and with regard to the rights and sensitivities of other people. Use must be in accordance with University policies and all relevant federal and state legislation.
3. Users shall not cause, or attempt to cause, security and/or privacy breaches or disruptions to telephone communications.
4. Harassment is not permitted, whether through language, images, videos, hang-up; silence; hoax; obscene; abusive; malicious or frequency and size of telephone, text or multimedia messaging calls. Users must not send unsolicited text messages, including "junk mail" or other advertising material.
5. Users who receive unwelcome calls must report these events, either by activating the MCID (Malicious Caller Identification) button on their phone, in which case IMTS will initiate an investigation, or by reporting the issue to IMTS or to the Complaints Management Centre in the Governance and Legal Division.
6. The recording of telephone calls is only permitted where this is done in accordance with relevant legislation, i.e. State and Commonwealth privacy laws and the Commonwealth Telecommunications Act. IMTS do not provide this service but are available to give advice on recording of telephone calls.
7. The University will use royalty-free music for the University's Music On-Hold.

5 Use of Mobile Devices

1. University Mobile Devices can be used for the following purposes:
    a. for making and receiving of all calls and messages, either work related or personal, provided non-University related usage is kept to a minimum and does not incur significant costs or loss of work time;
    b. for application and Internet use, either work related or personal, provided non-University related usage is kept to a minimum and does not incur significant costs or loss of work time.
2. For University staff who are frequently out of the office and have a University Mobile Device, it may be appropriate to forward calls from their fixed Telephone to their University Mobile Device.

As call charges are higher and will be charged back to the account holder's cost centre, prior approval from the relevant Senior Executive, Executive Dean or Director is required. The cost of forwarding fixed calls to a Mobile Device is automatically charged to the fixed Telephone account.

3. All individual outgoing call usage can be tracked and provided by IMTS on request by the User.
4. International data roaming is turned off by default, and activation of this service requires approval by IMTS. The User accepts all associated costs with the activation and usage of data roaming whilst overseas. Users may contact IMTS to find out available options for telephone contact while overseas.
5. All operating system updates and applications updates on devices covered under this policy must be applied, and a password/passcode must be used.
6. Users are required to contact IMTS if they require additional functionality (if available) for their Mobile Device account. Such requests will be subject to approval by the relevant Senior Executive, Executive Dean or Director.

6 Telephone and Mobile Device Accounts

Service Providers

1. University Telephones, Mobile Devices and Data Services must be connected to one of the IMTS recommended plans unless approval to use an alternative plan has been granted by the relevant Senior Executive, Executive Dean or Director and approved by the Director, IMTS.

Access to account usage information

2. The University has the right to capture and inspect any telephone call or account information made on a University Telephone or Mobile Device as per the conditions defined in the IT Acceptable Use Policy and in accordance with the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015.
3. Detailed Device 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 relevant Senior Executive, Executive Dean or Director made in writing and approved by the Director, IMTS or delegated persons, to investigate a potential breach of policy or for access to be granted;
    c. where deemed appropriate by the University in order to uphold the statutory rights of individuals in matters such as privacy, copyright, workplace health and safety, equal employment opportunity, harassment and discrimination;
    d. a proper request from an appropriate law-enforcement officer investigating an apparently illegal act, including a court order; or
    e. a relevant statute, specifically the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015.
4. All device account invoice information is securely retained by IMTS and access to account information will always be provided by persons nominated by the Director, IMTS. The University's policy and statutory legislation relating to privacy will be upheld in all cases. IMTS will provide an itemised invoice for a University account on request of the user of that Mobile Device.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

7 Mobile Devices

Acquisition

1. Purchase of Mobile Devices and SIM cards must be in compliance with the University Purchasing and Procurement Policy. Mobile Devices and SIM cards remain the property of the University.
2. Under no circumstances will the University cover the costs or obligations for Mobile Device plans entered into without approval of the relevant Senior Executive, Executive Dean or Director.
3. All staff authorised to acquire and use a University Mobile Device will purchase a device of the recommended standard configuration and model unless additional options are required and have been approved by the relevant Senior Executive, Executive Dean or Director. Information for purchasing devices is available from IMTS.

Care of Mobile Devices

4. Users must take due care when using University Mobile Devices and take reasonable steps to ensure that no damage is caused to any supplied equipment. Users must report any damage to the relevant Senior Executive, Executive Dean or Director who will determine the action to be taken. Users must not use equipment if they have reason to believe it is dangerous to themselves or others. Redundant devices or peripherals should be returned to IMTS for reuse or disposal through a designated recycling scheme.

8 Telephone Installation and Management

1. IMTS is responsible for the installation and management of Telephone/Voice Services, fixed line and mobile services.
2. Faults on the university Telephone/Voice Services are managed by IMTS and should be reported to IMTS for resolution.
3. IMTS is 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 or relocate a public telephone on the University premises.

9 Internal Voice / Data Services Management

1. A request for the provision of internal voice/ data services for an individual must come from the relevant supervisor and is based on login access linked to the individual's user account.
2. Non-login extensions will be issued for functions such as faxes, modems, and where a login extension is not suitable such as in the case of meeting rooms and shared offices. Requests for a non-login voice/ data service to be granted to an individual must outline the grounds for the request and be made by a relevant Senior Executive, Executive Dean or Director and approved by the Director, IMTS or Senior Manager, Client Services, IMTS.
3. Access rights for a voice/ data service can be applied for and requires approval from a relevant Senior Executive, Executive Dean or Director. Access rights are provided to allow national calls including mobile phones for login phones. Access rights for non-login phones allow local calls. The access rights of a voice service are scaffolded as follows:
    a. University internal access and (0)000 emergency only;
    b. access to the areas covered by the local telephone call district;

c. extensions with national access including mobile access; and

d. extensions with international access.

4. The ability to apply a call forward to an internal number is available by default, however call forwards to an external number including Mobile Devices require a request to be submitted to IMTS and will require approval from a relevant Senior Executive, Executive Dean or Director.

5. In cases where an extension requires more than one level of restriction, an additional level of authentication, namely pin code access via a Forced Activation Code (FAC) can be granted. FAC codes are linked to an individual's UOW user account. A FAC is created with specific access rights which override any handset restrictions that may apply.

6. Desk (fixed) Telephones are restricted from calling international destinations by default. A user can apply for approval to remove the international calling restrictions from their fixed Telephone permanently. Approval will be granted by the relevant Senior Executive, Executive Dean or Director.

7. The University does not permit the use of 1900, 1930 or 1300 numbers, except where a request is made in writing and approved by the Director, IMTS. IMTS have controls in place to block access to premium services in accordance with the Privacy Policy.

10 Administration and Implementation

Compliance

1. Telephone and Mobile Devices and accounts are issued on the basis that a user agrees to comply with the University's IT Acceptable Use Policy and this policy. Violations of the conditions of use of IT Facilities and Services may result in temporary or indefinite withdrawal of access, disciplinary action under the University's, or relevant entity's discipline procedures, and/or reimbursement to the University.

11 Roles & Responsibilities

1. The Director, IMTS can approve 1300, 1900, 1930 and other information services.
2. The relevant Senior Executive, Executive Dean or Director are responsible for:

    a. determining which staff are eligible for a Mobile Device and/or Mobile Device account and initiating their discretion to withdraw access rights;

    b. determining which staff or students are eligible for a fixed Telephone and the level of access for individual users;

    c. approving access to services which involve additional costs, such as International roaming and International dialling.

    d. ensuring Mobile Devices purchased are one of the recommended models from the University preferred supplier;

    e. ensuring that devices are managed as an asset and, if appropriate, included in the University Asset Register;

    f. monitoring use of devices by approved users in terms of unreasonable call charges and determine the level of personal call costs considered to be excessive; and

    g. notifying IMTS of changes when cancelling or re-assigning a device and/or account.

2. Individual Users are required to:
    a. read and abide by the Telephone and Mobile Device Use Policy;
    b. ensure the proper use, care and security of University devices and Mobile Data Services;
    c. report faulty, damaged, lost or stolen devices to IMTS immediately, and contact the service provider directly to block calls on the account if the device is stolen in or out of normal business hours;
    d. check to ensure their account charges are correct;
    e. identify personal call charges and reimburse the University if required;
    f. ensure the mobile telephone and/ or device is primarily used for University purposes; and
    g. return all Mobile Devices, complete with SIM card, if no longer employed by the University, the asset is no longer needed or if directed by the relevant Senior Executive, Executive Dean or Director. Additional accessories such as battery chargers must also be returned.
4. IMTS is responsible for:
    a. determining and updating the standard configurations for Mobile Device and data usage at the University;
    b. providing a system for the procurement of Mobile Devices by the University;
    c. creating and modifying Mobile Device accounts for approved users;
    d. paying Mobile Device or Data Service charges for accounts and services which have been approved for use by the relevant Senior Executive, Executive Dean or Director;
    e. debiting the nominated account monthly for the costs of approved Mobile, Devices and accounts; and
    f. providing itemised invoices for all accounts as requested.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

12 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	9 December 2016	University Council	First version, resulting from major review of IT Policy suite.
2	19 August 2020	Chief Operating Officer	Policy revision based on changes to technology and procedures.