UNIVERSITY OF WOLLONGONG AUSTRALIA

IT ACCEPTABLE USE POLICY

Date first approved: 1 July 2004	**Date of effect:** 1 July 2004	**Date last amended:** (refer Version Control Table)	**Date of Next Review:** December 2021
First Approved by:	Vice-Chancellor		
Custodian title & e-mail address:	Senior Manager Client Services, IMTS paul_morgan@uow.edu.au		
Author:	Cyber Security Manager, Infrastructure, IMTS Senior Manager Client Services, IMTS		
Responsible Division & Unit:	Information Management & Technology Services (IMTS)		
Supporting documents, procedures & forms of this policy:	Bullying Prevention Policy Copyright Policy Cyber Security Policy Fraud and Corruption Prevention Policy IT User Account Management Procedures Privacy Policy Purchasing and Procurement Policy Records Management Policy Research Data Management Policy Secondary Employment Policy Student Conduct Rules Telephone and Mobile Use Policy University Code of Conduct University Privacy Statement & Policy		
Relevant Legislation & External Documents:	*Crimes Act 1914* (Commonwealth) *Workplace Surveillance Act 2005* (NSW) *Criminal Code Act 1995* (Commonwealth) *SPAM Act 2003* (Commonwealth) *Copyright Act 1968* (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 University of Wollongong is committed to the appropriate use of Information Technology and Services to support its learning, teaching, research, administrative, and service functions. This policy defines acceptable behaviour expected of Users of University IT Facilities and Services. 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 (with examples if required)
Associate Account	Accounts that apply to individuals granted access to the University IT Facilities and Services by virtue of an affiliation with the University. Recognised affiliations are: - Contractors and consultants providing services to the University (typically involving a contract for services) - Visiting academics of the University other than those holding an honorary academic appointment - Members of the University Council - Members of a recognised business or community affiliate of the University of Wollongong
Computer Surveillance	Means surveillance, including by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, local or hard drive, public network, internet and email and other electronic technologies).
Enterprise Storage	Storage provided through IMTS that is protected from data loss.
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.
IMTS	Information Management & Technology Services at the University of Wollongong.
Staff	All persons appointed by the University as academic or professional services staff regardless of their level of seniority and regardless of whether holding full-time, part-time, or limited-term appointments, including conjoint appointments. For the purposes of this policy, it also includes all persons engaged by the University as casual employees
Student	A person enrolled in a course at the University of Wollongong.

University	University of Wollongong and controlled entities.
UOWmail	Office 365 for Students Services account provided by Microsoft under the Agreement for Email.
User	A person assigned a User Account by the University or a person who is otherwise authorised to use University IT Facilities and Services.
User Account	An identity assigned to a User, with an associated username, for the purpose of accessing IT Facilities and Services that require authentication by the user. Also referred to as account throughout this document.

3 Application & Scope

1. This policy applies to all use of University IT Facilities and Services. It covers computing, collaboration and communications facilities, examples of which include telephones, facsimiles, mobile telephones, computers, tablets, printers, photocopiers, email, internet access, network applications, web services and similar resources. Use of remote systems accessed via IT Facilities and Services is also covered by this policy. Remote services may have additional local rules and regulations.
2. Users must accept and comply with University IT policies as a condition of use. This policy is designed to allow legitimate and optimal use of IT Facilities and Services.

4 Policy Principles

1. IT Facilities and Services are provided to Users to conduct academic and administrative pursuits.
2. Users must take responsibility for using IT Facilities and Services in an ethical, secure and legal manner; having regard for the objectives of the University and the privacy, rights and sensitivities of other people.

Authorised Use, Access and Authentication

3. Users are authorised to use University IT Facilities and Services when assigneda User Account subject to the other conditions in this section. Authority to use IT Facilities and Services is not normally granted by other means. This does not apply to public services, which do not require authentication to access. All staff and students must have a User Account.
4. User Account creation and management is governed by the IT User Account Management Procedures.
5. Many IT Facilities and Services require authentication in order to access. Access is often further controlled based on roles, which are linked with the username of a User Account.
6. Some IT Facilities and Services are provided only for specific functions and may only be used by specifically authorised Users.
7. Users must use IT Facilities and Services only in the manner intended for their role.
8. Users must not share their User Account or password or other authentication credential. Users must not use an account assigned to somebody else. This does not apply where authorised IT

support staff are conducting their duties and the User has provid ed their credentials in the course of receiving support.

9. Users must set up the self-service password reset capability to assist when a password is forgotten or expired.
10. Users are discouraged from recording passwords on paper. A secure password management system is recommended if needed.

Security

11. Users have a responsibility to be vigilant and know how to protect themselves and IT Facilities and Services. Users must comply with the Cyber Security Policy.
12. Managed computers that are compromised will be reset to the standard image and software reinstalled by IMTS support staff.
13. It is important that all software on devices is up to date to ensure known security vulnerabilities are fixed.
14. Attackers use email to target Users. It is likely Users will encounter various forms of these popular threats.
    a. malicious email will attempt to entice Users to visit fake and forged websites to steal usernames and password.
    b. malicious email will attempt to persuade Users to open attachments that may lead to compromise of the device with malware.
    c. malicious email may encourage Users to take the first steps leading to a fraud scam.
15. Users must maintain awareness of current email threats, including taking care when reading email. The following advice will help protect against email attacks:
    a. Users should carefully check that the From and Reply-To addresses match the email address of the person the email appears to be from;
    b. Users should be alert to email that is prompting them to act urgently. Users should not act on any email which is unusual or out of the ordinary;
    c. Users should only open attachments from people who are trusted and from whom an email would be expected; and
    d. Users should avoid clicking through website links contained in email.. Where there is cause for suspicion the known site address should be typed into the browser or a search for the website undertaken.
16. Attackers use the web to target Users. Users must take care when browsing webpages. The following actions help protect against web attacks:
    a. browsers and all plugins must be kept up to date with security fixes;
    b. unnecessary browser plugins should be avoided;
    c. before authenticating to a website or entering private data, the security padlock and the legitimacy of the site address should be checked; and

d. software must not be installed if prompted. Software should only be installed if the User is authorised to do so and has deliberately downloaded the software from a trustworthy source.

17. The University uses various network and device security controls to help protect from cyber attacks. Occasionally these controls interfere with user experience, the University attempts to maintain an appropriate balance. Users must not subvert nor attempt to subvert any security control.
18. Access to a User Account may be temporarily suspended if the ac count is suspected to be compromised and is posing an unacceptable risk.
19. Users must not give means to a third-party to access IT Facilities and Services without approval from the IMTS Security Team.

Conduct and Activity

20. Users are responsible for the following whilst using the IT Facilities and Services:
    a. all activities that originate from their account;
    b. all information sent from, intentionally requested, solicited or viewed from their account; and
    c. information placed on a computer using their account.
21. Users must not use the IT Facilities and Services for the following activities.
    a. the creation or transmission (other than for properly supervised and lawful teaching or research) of any material or data that could reasonably be deemed abusive, offensive, defamatory, obscene or indecent;
    b. the creation or transmission of material that could reasonably be deemed likely to harass, intimidate, harm or distress;
    c. the unauthorised transmission of material that is labelled confidential or commercial in confidence; or
    d. deliberate unauthorised access to facilities or services.

Using Devices and Equipment

22. Users should exercise care when using IT equipment. Users will be held responsible for cost of repair if damage is caused through misuse or negligence. Damaged equipment that may cause harm must not be used. Damage to IT equipment must be reported to IT support staff.
23. IT Facilities and Services must not be tampered with or moved without authorisation.
24. When using computer laboratories. rules, signs and instructions from IT support staff must be complied with. Users must provide identification to support staff if requested.

Personally Owned Devices

25. Users may use a personally owned device such as a laptop, tablet or smart phone to access IT Facilities and Services on the following terms.
    1.1. Users may connect to the University Wi-Fi network or remotely access services via Internet.

1.2. Users must not connect a personally owned device to a wired network port without authorisation.

1.3. Users must comply with this Acceptable Use Policy.

1.4. Users must maintain good security hygiene of the device, including the following:

a. Turn on automatic updates and ensure software receives the latest fixes;

b. Use security software and configure security features such as firewall and anti-virus / anti-malware; and

c. Password protect their device.

1.5. A device must not be used where it is known to have a security compromise. Users must reinstall the operating system and all software from trustworthy sources before continuing to use the device.

1.6. Users must not store confidential or valuable University data on a personally owned device.

Cloud Computing & External IT Services

26. Procurement of externally hosted IT services must comply with the Purchasing and Procurement Policy.

27. Users must not store or backup confidential or valuable University data with externally hosted services other than where provided through and approved by IMTS.

Student Use of Software

28. Students are not allowed to install, attempt to install, copy, or download any type of software onto IT Facilities and Services, unless the student in an IT Laboratory specifically setup for the purpose of studying an IT related discipline where:

a. installation of software is required as part of the coursework;

b. there is proof the software license belongs to the University; or

c. the lecturer has given their authorisation.

29. Exceptions may apply to PhD research students using IT Facilities and Services provided to carry out their research. Any software that is to be instal led on these facilities must go through the normal software purchasing and approval mechanisms.

Non-University Use of IT Facilities and Services

30. The IT Facilities and Services are provided to support the University's teaching, research, administrative and services purposes.

31. The University accepts that Users will on occasion use IT Facilities and Services for incidental personal purposes. Users must balance use for personal purposes with the management of resources in an efficient, economical and ethical manner. They must ensure such use does not:

a. interfere with the operation of IT Facilities and Services;

b. interfere with other Users access to IT Facilities and Services;

c. burden the University with additional costs; or

d. interfere with their employment or other obligations to the University.

32. Users are not permitted to use the IT Facilities and Services for:
    a. unauthorised commercial activities;
    b. unauthorised personal gain; or
    c. unauthorised gain to a third-party.

Email and Internet Services

33. The University provides all Staff and Associate Accounts with a UOW email account.
34. The University provides students with a UOWmail email account. Students are required to comply with the UOWmail Conditions of Use when using their UOWmail account (see Appendix 1).
35. There are limits to the size of email items and the amount of email retained on servers, these may change from time to time.
36. There are limits to Internet data and bandwidth use, including web browsing activity, these may change from time to time.
37. The University may block or re-direct incoming email if they are deemed to be harassing or offensive to the recipient.

Telephones and Mobile Telephones

38. The use of telephones and mobile telephones must comply with this policy and with the Telephone and Mobile Use Policy.

Data

39. Users are responsible for appropriately handling University data and must comply with relevant University policies such as Privacy Policy, Intellectual Property Policy, Records Management Policy and Research Data Management Policy.
40. Users must consider security requirements of University data they create and access. If data is confidential, private or intellectual property requiring protection, it must be handled to avoid unintended disclosure. If losing data would incur a high cost or impact to the University, it must be handled to avoid accidental loss.
41. Technical controls (e.g. file permissions and authentication) must be used to restrict access to data only for authorised Users.
42. Data storage solutions provided by IMTS are suitable for storing both confidential and valuable data. These solutions are accessed via the network, have authentication and access controls, and provide a high level of protection from data loss by maintaining copies in multiple sites and use highly redundant technology. Current solutions are referred to as central file shares, home drives (H drive) and shared drives (S drive).
43. Confidential data must not be stored on external or portable drives.
44. Confidential or valuable University data must not be stored on personally owned devices.
45. Confidential or valuable University data must not be stored on cloud services or externally hosted services other than where the service is provided through and approved by IMTS.

46. Users must only examine, disclose, copy, rename, delete or modify data if they are authorised to do so. This includes stored data and when in transit via a network.
47. Obsolete devices which have stored confidential data, must be disposed of securely to avoid accidental disclosure. Users should consult with IMTS for advice before proceeding with such activity.

Data Backup

48. Valuable University data must be stored to avoid accidental loss. It is not sufficient to rely on storage devices in desktops, laptops, external/portable drives, tablets and telephones to store valuable data.
49. All valuable University data must be primarily stored (or have a current copy stored) on enterprise storage provided through IMTS.
50. It is common for user devices to fail and cause loss of all data stored on the device. Be aware that the hard drive, desktop and 'my documents' folders are not automatically backed up. Users must maintain current copies of valuable data on enterprise storage systems.

Copyrighted Software and Content

51. Users are responsible for making use of software and electronic materials in accordance with the Copyright Act 1968 (Commonwealth), software licensing agreements, and any applicable University policies including the Copyright Policy.
52. Unauthorised copying or communication of copyright protected material (includng music and videos), violates the law and is contrary to the University's standards of conduct and business practices. The University will enforce controls within the institution to prevent the copying or use of unauthorised music, videos, and software. This includes effective measures to verify compliance with these standards.

Dealings in Copyright Protected Material for Teaching or Research

53. Staff and students can copy and or communicate copyright protected material for teaching or study purposes where they have the permission of the copyright owner. Limited permission may be granted, for example, via website statements, license agreements, or under the statutory license provisions of the Copyright Act, 1968 (Commonwealth).
54. Staff and students may also be able to copy limited portions of material under the 'fair dealing' provisions of the Copyright Act, 1968 (Commonwealth).
55. For more information on what, and how much, users can copy and communicate under the fair dealing and statutory license provisions of the Copyright Act, 1968 (Commonwealth) see http://www.library.uow.edu.au/copyright/index.html

Privacy

56. The University seeks to comply with privacy requirements and confidentiality in theprovision operation of all IT Facilities and Services. Users must comply with the Privacy Policy whilst using IT Facilities and Services. For further information refer http://www.uow.edu.au/about/privacy/index.html

57. User's names and usernames will be listed in directories accessible to other Users for the purpose of enabling collaboration. Users may apply to use an alias for this purpose where they have reasonable privacy concerns.
58. Users must be aware that unless encrypted, stored data and data in transit via the network may be able to be accessed by unauthorised persons. Users should use secure network protocols for transferring data on the internet.
59. When using a multi-user system such as shared Solaris OS computer, users must be aware that many of the activities undertaken may be visible to other Users. For example, session start and end times; origin of session; as well as commands and command arguments executed.
60. Logs of User activity are maintained by IMTS for troubleshooting, accounting, security investigations, reporting and legal purposes. These logs include times of sent and received email; email addresses (both sender and recipient), network activity metadata, web sites visited, telephone call records, files read or written; and computers and services accessed. These logs are stored securely and are retained for at least 2 years.
61. Be aware that unforseen security weaknesses or failures may result in a determined person accessing private or confidential data. Additionally, authorised IT staff may incidentally observe data during the course of their duties.

Computer Surveillance

62. The University will conduct ongoing and intermittent Computer Surveillance of all Users and devices which access the IT Facilities and Services for the purpose of:
    a. protecting its assets, property and finance from suspected unlawful activities or activities which are in breach of University Policy or Rules;
    b. conducting its business and operational requirements;
    c. protecting its reputation;
    d. compliance with legislative requirements; and
    e. meeting the expectations of stakeholder and the general public
63. The University is committed to meeting its statutory obligations under the Workplace Surveillance Act 2005 (NSW) and this IT Acceptable Use Policy represents formal notification to Users about activities of the University that fall within the definition of Computer Surveillance.
64. Computer Surveillance will be carried out by all means available to the University including but not limited to:
    a. accessing University email accounts or emails;
    b. accessing files;
    c. accessing work computers, including activity logs;
    d. recording internet usage (including sites and pages visited, files downloaded, video and audio files accessed and data input) and accessing these records;
    e. accessing telephone usage logs; and

f. accessing personal devices that have been used to conduct University business.

65. Users acknowledge that Computer Surveillance may prevent, or cause to be prevented:
    a. delivery of an email sent to or by a User;
    b. access to an internet website; or
    c. access to software applications.
66. The University will notify the User as soon as practicable that an email has not been delivered except where:
    a. the email was a commercial electronic message within the meaning of the SPAM Act 2003 (Commonwealth);
    b. the content of the email or any attachment to the email would or might have resulted in an unauthorised interference with, damage to or operation of a computer or computer network operated by the employer or of any program run by or data stored on such a computer or computer network;
    c. the email or any attachment to the email would be regarded by a reasonable person as being, in all circumstances menacing, harassing or offensive; or
    d. the University was not aware (and could not reasonably be expected to be aware) of the identity of the employee who sent the email or that the email was sent by an employee.
67. The University will not prevent delivery of an email or access to a website merely because:
    a. the email was sent by or on behalf of an industrial organisation or employees or an officer of such an organisation; or
    b. the website or email contains information relating to industrial matters.
68. The University has a legitimate right to capture and inspect any data stored or transmitted on the University's IT Facilities and Services and personally owned devices including data of a private or personal nature (regardless of data ownership), when investigating system problems or potential security violations, and to maintain system security and integrity, maintain business continuity, and prevent, detect or minimise unacceptable behaviour on that facility. Such data 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 Executive, Executive Dean or Director to investigate a potential breach of policy;
    c. circumstances where it is deemed appropriate by the University for the purpose of business continuity, a request from the Executive, Executive Dean or Director,
    d. circumstances considered by the University to be sufficiently exceptional to warrant the release of the data;
    e. circumstances where it is 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;
    f. a proper request from an appropriate law-enforcement officer investigating an apparently illegal act, including a court order; or

g. a relevant statute.

69. Access to data will only be granted following a request from the Executive, Executive Dean or Director, made in writing and approved by the Director, IMTS or delegated persons.

70. Access to any data will always be via network or systems administrators, or via persons nominated by the Director, IMTS. The University's policy and statutory legislation relating to privacy will be upheld in all cases.

5 Administration and Implementation

Compliance

1. This compliance section is relevant and enforceable across all IT Policies.
2. The University treats misuse of its IT Facilities and Services seriously. 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 demand for reimbursement to the University.
3. IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Finance 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.
4. In the case of misuse of IT Facilities and Services by a staff member of a controlled entity or affiliate, a User's access will be withdrawn following a written request from the relevant Director/CEO of the controlled entity or affiliate. Access may also be withdrawn by IMTS in response to a suspected policy violation. A User whose access has been withdrawn may request reconsideration of the decision by the Director, IMTS who shall consider the withdrawal in consultation with the relevant controlled entity or affiliate. Following this, the Director, IMTS shall confirm the withdrawal or reinstate access.
5. Misuse or unauthorised use of University IT Facilities and Services may constitute an offence under the Crimes Act, 1914 (Commonwealth) and/or other pieces of State or Commonwealth legislation. Nothing in this policy 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.

6 Purpose of Policy

1. Roles and Responsibilities are as detailed throughout this Policy and in the Cyber Security Policy.

UNIVERSITY OF WOLLONGONG AUSTRALIA

7 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	1 July 2004	Vice-Chancellor	Policy converted into new ITS policy format. Addition of point re subverting restriction or accounting controls in Section 4 (point 8) Revised compliance statement to conform to the new Rules for Student Conduct. Compliance section under Administration and Implementation changed to include a reference to reimbursement to the University. Improved links to other policies Revised software and electronic materials section in line with the Music, Video and Software Piracy Policy. Completed the "Rules Governing the Use of IT Facilities" as an appendix to this policy. These are an extraction of the adopted IT policies and replace the now obsolete "Rules governing the use of University computer facilities". Removed appendix for email etiquette and rules governing the use of computer laboratories from this document.
3	1 September 2004	Vice-Chancellor	ITPAC and IT Forum approved version
4	15 November 2005	Vice-Chancellor	Included p2p example under General Principles Point 8.
5	6 May 2009	Vice-Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh Renamed the Rules Governing the Use of It Facilities as "Requirements Governing the Use of IT Facilities."
6	9 March 2010	Vice-Principal (Administration)	Future review date identified in accordance with Standard on UOW Policy
7	19 March 2013	Finance and Resources Committee	Revised and updated policies approved by Finance and Resources Committee.
8	4 November 2013	Chief Administrative Officer	Updated to reflect title change from University Librarian to Director, Library Services.
9	30 January 2014	Vice-Chancellor (VCAG)	Updated University nomenclature
10	9 December 2016	University Council	Major review of IT Policy suite

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Appendix 1 – UOWmail

1 UOWmail Conditions of Use

1. The University has entered into the Office 365 for Students Microsoft Volume Licensing Online Services Use Rights ("the Agreement") with Microsoft to provide UOWmail accounts. This means your UOWmail account is an Office 365 for Students Service Account.
2. The University has obligations under the Agreement with Microsoft to ensure that any User complies with the following terms and conditions in accessing and using their UOWmail account.

2 Definitions

Alumni	a graduate or former student of the University
Microsoft	Microsoft Corporation
Microsoft Services	(collectively) the Office 365 for Education
Password	the password associated with the UOWmail account
Student	a person enrolled to study or registered for a course at the University.
UOWmail	the Office 365 for Students Service provisioned by the University to provide E-mail Services
University	University of Wollongong
User	any Alumni, Student, or other individual associated with the University who is authorised to access and use UOWmail and Users shall be interpreted in the same way

3 Email Services

1. The University provides Users with a UOWmail account to enable communication on study and University related matters.
2. Users acknowledge that they cannot delete their UOWmail account until they are no longer enrolled at the University and their UOW user accounthas been deleted in accordance with the UOW IT User Account Management Procedures which can be accessed at http://www.uow.edu.au/about/policy/it/index.html. At this time a User must request to have their UOWmail account deleted. Alternatively, the User's account will be deleted in accordance with the IT User Account Management Procedures.
3. Users acknowledge that the University cannot guarantee continuous access to the UOWmail due to IT system maintenance and unplanned outages.
4. Users acknowledge that Microsoft may filter UOWmail accounts for spam and other malware and block access or prevent delivery of communications in order to protect itself, its customers or to prevent a breach of the Agreement.

5. Users acknowledge that Email is not a secure means of communication. While the University and Microsoft will both use best endeavours to ensure the security of their IT systems, this cannot be guaranteed particularly when communicating with parties external to the University.
6. Any User under the age of 16 must provide the University with written consent from their parent or guardian before the University can grant access to a UOWmail account. The consent must expressly authorise the provision of a U OWmail account in accordance with the UOWmail Conditions of Use.

4 Privacy

1. Users consent to the University providing their name, UOW user account name and Password to Microsoft for the purpose of access and management of UOWmail. The University will only disclose personal information to Microsoft as required to provide the User with a UOWmail account.
2. Users agree and acknowledge that any personal information collected by Microsoft may be transferred outside Australia and stored and processed overseas.
3. Users agree and acknowledge that Microsoft may need to disclose their personal information in order to comply with the law.
4. Users acknowledge that in dealing with personal information Microsoft's privacy practices and policies comply with the relevant provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Privacy Act 1998* (Commonwealth).

5 Passwords

1. Users understand that their UOWmail Password is synchronised with their UOW user account password whenever their UOW user account is active. Users can change their Password in UOWmail however the next time a User changes their UOW user account password it will automatically change their Password in UOWmail.
2. Users understand that when they are no longer enrolled as a student of the University, their UOW user account is closed and rendered inactive in accordance with the UOW IT User Account Management Procedure which can be accessed at:

   http://www.uow.edu.au/about/policy/it/index.html

3. At this time their UOWmail account Password will no longer be synchronised with their UOW user account password.
4. Users are responsible for the use of their UOWmail Password. Users should keep their Password secure and not disclose it to anyone.

6 Suspension and Termination of UOWmail Account

1. Users agree and acknowledge that Microsoft may suspend or terminate the provision of their UOWmail account if the User has engaged in any of the following activities:
   a. engaged in, facilitated or furthered unlawful conduct;

b. used the Microsoft Services in a way that harms Microsoft or Microsoft 's advertisers, affiliates, resellers, distributors and/or vendors, or any customer of Microsoft or Microsoft's advertisers, affiliates, resellers, distributors and/or vendors;

c. used any portion of the Microsoft Services as a destination linked from any unsolicited bulk messages or unsolicited commercial messages ("spam");

d. used any automated process or service to access and/or use the Microsoft Services (such as a BOT, a spider, periodic caching of information stored by Microsoft, or"meta-searching");

e. damaged, disabled, overburdened, or impaired the Microsoft Services (or the network(s) connected to the Microsoft Services) or interfere with anyone 's use and enjoyment of the Microsoft Services; or

f. resold or distributed the Microsoft Services, or any part of the Microsoft Services.