Email and Internet Policy

Section 1 - Purpose and Context

(1) Internet and Email services are vital to Western Sydney University's (the University) ability to function as a modern higher learning institution and to further its vision, mission and goals. However, these services can be misused, either accidentally or intentionally, without a framework to provide guidance for how the University expects these services to be used. Certain legal requirements, ordinary lines of management and approval, as well as general standards of respect and courtesy apply to email and internet usage to the same degree as any other piece of University formal business or communication activity.

(2) This policy and the associated Procedures and Guide documents provide a framework for the appropriate, effective and efficient use of University email and internet services. In addition to general usage principles, the policy also addresses related issues of privacy, confidentiality, security, and Authorised Users' legal obligations.

(3) This policy applies to all Authorised Users of University email and internet (wired or wireless).

(4) In compliance with the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth), the University does not provide anonymous internet access, but may establish third party ISP services available for events or specific arrangements.

(5) Use of University email and internet service is expected to follow all other relevant University policies, in particular:

a. Acceptable Use of Digital Services Policy
b. Workplace Surveillance Policy
c. Code of Conduct
d. Student Misconduct Rule
e. Email and Internet Procedures
f. Email and Internet Guide

Section 2 - Definitions

(6) Words and terms used in this policy are defined in Section 6 — Terms and Acronyms.

Section 3 - Policy Statement

(7) University Email, both accounts and messages, remains the property of the University. All University staff, students, and some associates of the University are provided with access to an individual University email account for the purposes of sending and receiving official emails related to the business of the University or the student's enrolment and program of study.

(8) When Authorised Users leave the University, their User accounts—including documents, emails and internet access (and records of access)—are archived and retired. This means that ex-staff and -students will not have access to their user accounts or emails after leaving. Therefore, before leaving the University, users are responsible for:

a. tidying their own documents and mailboxes;
b. ensuring their managers or teams have the necessary information to safeguard business operations;
c. making copies of any personal information that they will require;
d. contacting any internal or external correspondents to make them aware that the University email address will be retired (see the Staff Separation Checklist or ServiceNow Knowledge Article 0012730 – Staff Off-Boarding for more details); and
e. ensuring University Intellectual Property remains with the University. While copies of personal data are acceptable, University business remains university property; no departing Authorised User is permitted to take any University Digital Information. See the Intellectual Property Policy for more information.

(9) Before leaving, staff are welcome to inform personal contacts of an appropriate new email address, to avoid bounce messages. Upon leaving, staff should add an Out of Office message indicating that they are no longer working in the position they occupied, and that their manager should be contacted for university business. However, a User leaving a forwarding message containing their new position and/or email address is not appropriate, as staff email accounts are intended for University business. Refer to KB0012730 ServiceNow for further information.

(10) University provided internet access is generally made available to all Authorised Users to conduct business, study and research. All Authorised Users, including Eduroam users, are required to adhere to the Acceptable Use of Digital Services Policy.

(11) The University distributes important information, formal notices and other official communications via University email accounts and expects staff and students to check their account and read their University email regularly. The University acknowledges that the use of email can increase pressure on workplaces through the large number of emails sent to some staff and the unrealistic expectation of an immediate reply.

(12) If any Authorised Users, including Eduroam users, breach the terms of this policy, their access to the University Digital Services may be limited or revoked, and the matters may be referred to the relevant internal or external authorities if the University deems it necessary.

(13) The University endeavours to maintain the security of University email and internet but it cannot guarantee confidentiality, or undiscovered interception or alteration of communications (whether via email or interactions with internet sites and services) by third parties.

(14) Emails sent by staff members of the University, especially when acting in their official capacity, should include a signature line in keeping with the University's branding resources (requires staff login). Staff are advised that disclaimers or other common signature line messages are able to be added as described in the branding resources.

(15) Incidental and occasional use of University email for personal use is acceptable. However, use of the email system as a personal email solution is not authorised.

Authority of ITDS to Restrict Access

(16) As defined in the Workplace Surveillance Policy, the University is not required to give notice of emails being blocked if:

a. the University regards the content of the website or email, including any attachment, as menacing, harassing or offensive, for example, pornographic, gambling, or terrorist websites;
b. the email is or contains a commercial electronic message, as defined in the Spam Act 2003(Commonwealth);
c. the content or attachments of the email would or might result in unauthorised interference with, damage to, or operations of a Digital Service (including any program run or data stored on any Digital Service);
d. the sender of the email has been identified as having previously sent malicious content to the organisation;

e. the University is not aware (and cannot reasonably be expected to be aware) of whether an employee has sent that email or of the identity of the employee who has sent that email.

(17) A breach of this policy will be dealt with in accordance with the relevant staff employment agreement, the Student Misconduct Rule, the Code of Conduct and/or University policy.

Section 4 - Processes

(18) See the Email and Internet Procedures document.

Section 5 - Guidelines

(19) See the Email and Internet Guide document.

(20) This policy should be read in conjunction with the following:

a. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)
b. Spam Act 2003 (Cth)

Section 6 - Terms and Acronyms

(21) The following definitions apply for the purposes of this policy:

a. Authorised User: a person who is a currently enrolled or attending student, a current employee, or a formal supplier, joint venture partner, affiliate or associate of the University who is granted access and provided with authentication Credentials by the University. Eduroam users are also Authorised Users.
b. CIDO: Chief Information and Digital Officer
c. Digital Services: synonymous with IT Resources; all services (e.g., data, voice, video) delivered through electronic means. This includes the capture, storage, retrieval, transfer, communication and/or dissemination of information electronically and the technologies used in support of these activities. Such technologies encompass systems, software, hardware, communications and network facilities. The method of delivery may be hosted within University IT facilities, externally or a combination. They may be paid or free, subscribed or purchased, provided through a cloud or as a managed service.
d. Eduroam: An educational roaming internet service offered by multiple organisations worldwide, including Western Sydney University. This provides University staff and students access to internet through Eduroam when at another member's campus/facility.
e. Eduroam user: a person granted Eduroam access and credentials by an Eduroam organisation (such as Western Sydney University). Eduroam users are Authorised Users and granted access to the University's internet.
f. Email: a message, including any attachments, in an electronic format that is sent from one person to one or more other persons via a computer network using an email protocol (such as SMTP, IMAP).
    i. Official Email: any email sent or received that relates, even peripherally, to work for or study with the University, including its functions, goals, interests, or business.
    ii. Personal Email: email sent or received through University IT systems that is relevant to the personal matters of the sender and/or receiver but not relevant to the University in any way.
    iii. University Email: the official email service the University provides to staff and students, including the content of emails, electronic attachments to emails and transactional information associated with such communications. University email is a Digital Service and is the property of the University. University emails are emails sent or received using a University email account.

g. ISP: Internet Service Provider
h. ITDS: Information Technology and Digital Services
i. IT Resources: refer to Digital Services.
j. IT Service Desk: a team within ITDS, established to be the first point of call for staff and students, for all IT matters.
k. Phishing: a form of social engineering, commonly an email or telephone call, designed to convince Users to provide information about or access to a Digital Service; believing the source of the message to be genuine, or originating from within that Digital Service.
l. Spam: an email that is:
    i. unsolicited; and
    ii. sent to a large number of email addresses; and
    iii. does not relate to University business; OR
    iv. defined as Spam under the Spam Act, 2003.
m. University Email Address: an email address that includes a domain name of the university or one of its related entities (for example; name@westernsydney.edu.au)
n. University Internet: any internet connectivity provided to Authorised Users by the University, including:
    i. wired, wireless, and mobile internet; and
    ii. all online activity and all information uploaded and downloaded.

Status and Details

Status	Current
Effective Date	20th December 2019
Review Date	3rd January 2022
Approval Authority	Vice-Chancellor and President
Approval Date	20th December 2019
Expiry Date	Not Applicable
Unit Head	Scott Snyder Chief Information and Digital Officer s.snyder@westernsydney.edu.au
Author	Anita King 45701708
Enquiries Contact	Anita King IT Assurance Specialist 45701708