

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 resources can be misused, either accidentally or intentionally, without a framework to provide guidance for how the University expects these resources 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 formal business or communication activity.

(2) This policy and the associated Procedures and Guidelines documents provide a framework for the appropriate, effective and efficient use of University email and internet resources. 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) Use of University email and internet resources is expected to follow all other relevant University policies, in particular:

- a. [Acceptable Use of Digital Services Policy](#)
- b. [Digital Information Security Policy](#)
- c. [Code of Conduct](#)

Section 2 - Definitions

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

Section 3 - Policy Statement

(6) 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.

(7) 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 IT Resources Policy](#).

(8) 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.

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

(10) 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.

Authority of ITDS to Restrict Access

(11) 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 an IT Resource (including any program run or data stored on any IT Resource);
- 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.

(12) A breach of this policy will be dealt with in accordance with the relevant staff employment agreement, the [Student Misconduct Rule](#), and/or University policy.

Section 4 - Processes

(13) See the [Email and Internet Procedures](#) document.

Section 5 - Guidelines

(14) See the [Email and Internet Guide](#) document.

Section 6 - Terms and Acronyms

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

- a. Authorised User: a person who is an enrolled or attending student, a current employee, or a formal supplier, 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. 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.
- d. 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.
- e. 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 an IT Resource and is the property of the University. University emails are emails sent or received using a University email account.
- f. ISP: Internet Service Provider
- g. ITDS: Information Technology and Digital Services
- h. IT Resources: systems, software, hardware, services, communications and network facilities (including email, internet, and Wi-Fi access), and supporting infrastructure provided by or on behalf of the University.
- i. [IT Service Desk](#): a team within ITDS, established to be the first point of call for staff and students, for all IT matters.
- j. Phishing: a form of social engineering, commonly an email, webpage pop-up, or telephone call, designed to convince Users to provide information about or access to an IT system; believing the source of the message to be genuine, or originating from within that IT system.
- k. 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](#).
- l. University Email Address: an email address that includes a domain name of the university or one of its related entities (for example; j.bloggs@westernsydney.edu.au)
- m. 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	Historic
Effective Date	12th April 2017
Review Date	12th April 2019
Approval Authority	Vice-Chancellor and President
Approval Date	11th April 2017
Expiry Date	19th December 2019
Unit Head	Bianca Jordaan Chief Information Officer b.jordaan@westernsydney.edu.au
Author	Anita King 45701708
Enquiries Contact	Bianca Jordaan Chief Information Officer b.jordaan@westernsydney.edu.au