WESTERN SYDNEY
UNIVERSITY

Email and Internet Guide

December 2019

Section 1 - Purpose and Context

(1) These guidelines provide information to assist students and staff to understand their rights and responsibilities while using Email and Internet services. These guidelines should be read in conjunction with the Email and Internet Policy and Email and Internet Procedures.

Section 2 - Definitions

(2) Refer to the Email and Internet Policy.

Section 3 - Policy Reference

(3) Refer to the Email and Internet Policy.

Section 4 - Procedures

(4) Refer to the Email and Internet Procedures.

Section 5 - Guidelines

Relevant Legislation and Users' Obligations

(5) A listing of relevant legislation is provided on the Associated Information page of the Email and Internet Policy. This section is intended to provide guidance to Authorised Users of University email and internet.

(6) The immediacy and convenience of email and the ability to use it to contact a wider group of people can also make it easier to inadvertently breach the law. It is important to note that even deleted emails can be forensically retrieved.

(7) Email is subject to the laws and protocols applying to other communications including copyright, breach of confidence, defamation, privacy, contempt of court, anti-discrimination legislation, as well as the creation of contractual obligations and criminal law. Any communication conducted across the internet, including textual, auditory, visual, or any combination of these is subject to the same laws and protocols. See the Copyright Policy for more information.

(8) University Records (including emails forming part of the University's record) can be accessed under the Government Information (Public Access) Act, 2009 (NSW), or through an order of a court or tribunal.

(9) Where email is sent and received by an employee who is acting in their University capacity, it forms part of the official records of the University. As part of its record-keeping and archival policy, the University expects all emails that are identified as records, under the State Records Act, 1998 (NSW), to ensure they are appropriately archived in the TRIM system; thus ensuring that accountability, audit and legislative requirements are met. Emails should not be deleted prior to them being archived in the TRIM system, so that minimum retention requirements are applied to the record. For more information, see the Records and Archives Management Policy.

(10) This policy does not address the ownership of intellectual property stored in or transmitted via University resources (including email and internet) as this is governed by the Intellectual Property Policy.

(11) Personal information is defined in the Privacy Act, 1988 (Cth), the Privacy and Personal Information Act, 1998 (NSW), and the Health Records and Information Privacy Act, 2002 (NSW). Personal information includes any information or opinion with which

the person's identity can be reasonably guessed, as well as finger print, retina scans, and genetic characteristics. Health information also includes physical and mental health or disability, health care service provided and the person's wishes about future health care. Unless this information is already public (via disclosures, declassifications, and so forth), the University, its staff, and students have a responsibility and legal obligation to prevent any personal information from unauthorised release. See the Privacy Policy and the Privacy Management Plan for more information.

(12) Any unauthorised access to or modification of data held in a computer with the intent to commit a crime is an offence under the Cybercrime Act, 2001 (Cth). If a User of University IT Resources finds they have accidentally accessed information they are not supposed to have access to, they should report this to the IT Service Desk immediately. See the Cyber Security Policy for more details.

Email Guidelines

(13) The following information is provided as a guide to facilitate efficient use of University Email resources:

Distribution and Addressing of Emails

(14) Authorised Users should:

a. determine the appropriate person to whom an email is to be sent. Forwarding emails to a number of people can lead to uncertainty as to the responsibility for action, double handling, wasted time, lost information, delayed responses and general frustration.

b. keep emails within their appropriate channel of decision making as this promotes efficient and effective management.

c. address the email only 'TO' those people who are required to take some action in the matter. The 'CC' field should be used for those people to whom the email is sent only for information purposes; or

d. include an appropriate note in either the subject or at the beginning of the message where an email is being sent for information purposes only. This can be done either by stating that the message is "For your information" or "No action is required on your part".

Subject and Content of Emails

(15) Authorised Users should:

a. ensure that the subject and content of an email is concise and meaningful.

b. ensure that the subject of the email is directly related to the body content.

c. avoid sending single emails covering multiple unrelated matters.

d. ensure that the tone and content of an email is consistent with the professional tone and practices appropriate to University communications.

e. identify themselves clearly in all University Emails that they send. For example, all staff should consider including include their name, job title, telephone numbers and physical address at the end of the email message, as outlined in the University Email Signature Templates (staff login required).

f. When University Email Resources are used for personal purposes, ensure that it is made clear to any recipient that the email is not being transmitted by an Authorised User in any capacity as a representative of the University.

g. Ensure emails that are considered University records are appropriately stored in the TRIM system. See Clause 9 and the Records and Archives Management Policy for more details.

Internet guidelines

(16) The following information is provided to facilitate the effective and efficient use of University Internet Resources:

a. The perceived increase of anonymity afforded by the internet can cause other people to feel that they should behave inappropriately, just to see what kind of reaction they can provoke.

   i. If Authorised Users believe they are in this situation, they are advised to ignore obviously inaccurate or insulting messages.

   ii. Access to and use of University resources is logged, and any acts of bullying, discrimination, harassment, vilification, victimisation or inappropriate behaviour can be reported via the steps outlined in the Discrimination, Harassment, Vilification and Victimisation Prevention Policy and Bullying Prevention Policy.

b. Ads on websites will often attempt to disguise themselves to look like a legitimate part of the main website. Authorised Users are advised to look for 'Ads by…' or 'Advertisement' labels if they are unsure about a link.

c. When using a public computer to access a website or online system that requires a password or Credentials, Authorised Users are advised to log out of that website or online system before closing the web browser, as others could access the website or online system after you have left the computer. Authorised Users should also ensure Credentials and other form data is not cached.

General Information

(17) Staff are advised to consult the separation checklist for more information on archived email, capturing emails that are University records to the TRIM system, and taking copies of personal information they will require after leaving the University. Staff are permitted to make copies of personal email and personal information concerning themselves, however:

a. University business remains property of the University (see the Intellectual Property Policy for more details); and

b. There is a legal obligation separate from any University policy not to divulge personal or sensitive information without permission, even after leaving the University's employment (see the Privacy Management Plan for more details).

(18) Consider embedding video clips into presentations, where possible and legal to do so, instead of linking to them. This can help eliminate lag at presentation times, as Internet resources will not be required.

Things to Avoid

(19) When using University Email and Internet Resources, Authorised Users should avoid:

a. activities that place an unnecessary strain on University Email or Internet Resources (e.g., streaming video, playing games or sending mass emails during business hours);

b. activities that are better suited to an alternate form of communication. For example, the use of email to deal with disputes and difficult situations should be avoided. Personal face-to-face communication is a better, more collegial model for solving problems and creating a positive work climate;

c. activities that are or might be perceived as harassing in nature. This would include emails that:

   i. incorporate non-inclusive language,

   ii. have a harassing tone, or

   iii. are sent at an unreasonable rate or frequency, for example where the respondent is not given a reasonable time to respond. See the Discrimination, Harassment, Vilification and Victimisation Guidelines for more details on avoiding language that might be perceived as harassing in nature;

d. soliciting large volumes of incoming email that is not directly relevant to their role. Authorised Users may be required to unsubscribe from external mailing lists if they consume large amounts of bandwidth, storage space or otherwise compromise the University IT Environment; and

e. unrealistic expectations for expediency. Users should not infer that a greater priority will be given to email requests over other forms of communication, requests for information or assistance.

Reference Information

(20) These guidelines are to be read in conjunction with the following University documents:

a. Copyright Policy

b. Cyber Security Policy

c. Email and Internet Policy

d. Email and Internet Procedures

e. Intellectual Property Policy

f. Privacy Policy

g. Privacy Management Plan

h. Discrimination, Harassment, Vilification and Victimisation Prevention Policy

i. Bullying Prevention Policy

j. Records and Archives Management Policy

k. University Email Signature Templates (staff login required)

l. KnowledgeBase article KB0012730 (Staff separation | ITDS requirements)

m. The staff separation checklist

(21) These guidelines are to be read in conjunction with the following legislative documents:

a. State Records Act, 1998 (NSW)

b. Privacy Act, 1988 (Cth)

c. Privacy and Personal Information Act, 1998 (NSW)

d. Health Records and Information Privacy Act, 2002 (NSW)

e. Cybercrime Act, 2001 (Cth)

f. Government Information (Public Access) Act, 2009 (NSW)