IT Appropriate Use - Email Procedure

Section 1 - Summary

(1) The purpose of this Procedure is to provide information and advice on the proper use of the University's email service and to inform users of the University's required standard for email use.

Section 2 - Scope

(2) This Procedure applies to VU employees, students and other authorised users on both onshore and offshore locations with access to a University email account.

Section 3 - Policy/Regulation

(3) IT Appropriate Use Policy

Section 4 - Procedures

Part A - Summary of Roles and Responsibilities

Roles	Responsibilities
Employees, students and authorised users	VU email services must be used in responsible, professional, effective and lawful manner.

(4) All email accounts maintained on the University's email systems are the property of VU.

(5) The use of University email services including the sending and forwarding of emails must comply with this Procedure, the IT Appropriate Use Policy and other relevant University rules, policies and procedures, including:

a. the Information Security Policy and Information Security - User Access Management Procedure;
b. the Appropriate Workplace Behaviour Policy, Student Conduct Policy and Student Charter; and
c. the Bullying Prevention and Management Policy, Sexual Assault Response Policy, Sexual Harassment Response Policy, and the Discrimination and Harassment Prevention and Management Policy; and
d. the Copyright Policy.

Part B - Email Procedures

(6) VU email accounts should be used for sending all University-related email communications both internally and to external organisations.

(7) The University uses email as the primary method of communication with employees and students including urgent and time-critical information and announcements. Employees and students are required to check their VU email

account on a frequent and consistent basis and respond to calls to action in a timely manner.

(8) All emails sent from University staff email accounts must be classified according to the Information and Asset Classification Framework based on information contained within the email body and/or attachments. See confidential and restricted emails section for more additional information.

(9) A disclaimer will be automatically attached to all outgoing emails sent from University email accounts. This disclaimer must not be altered or interfered with in any way.

(10) Employees leaving the University will not have access to their email account after end of employment. It is the employee's responsibility to ensure any necessary information to maintain business operations is handed over to their managers or teams prior to departure.

(11) Requests to setup a new shared mailbox or access an existing shared mailbox can be made through the VU Support Hub and requires appropriate approval.

(12) Requests for delegate access to another employee's mailbox can be made through the VU Support Hub and requires appropriate approval from the mailbox owner.

(13) Requests to delegate mailbox access to another employee when leaving the University requires approval from the mailbox owner and their supervisor or manager.

(14) Emails can be sent on behalf of another user as long as the user has given the appropriate approval and permissions.

(15) Emails sent from VU email accounts must not contain customised backgrounds. Backgrounds should remain as a default that is provided by the email applications.

(16) Employees should follow Best Practice Email Guidelines when sending and replying to emails using their VU email account.

Part C - Unauthorised Actions

(17) The following actions are not allowed by law when sending or forwarding emails:

a. Using material which constitutes an infringement of copyright. Refer to the University's ' Copyright Policy in determining what third party material can be used.
b. Defaming an individual, organisation, association, company or business.
c. Communications that are obscene, offensive or involve the use of illegal material, including the use or transfer of material of a sexual nature.
d. Breaching a university policy, procedure, statute or regulation.
e. Directly or indirectly interfering with or conflicting with lawful University business.
f. Intentionally bringing the University or its officers into disrepute.
g. Sending unsolicited and unauthorised global or commercial email messages.
h. Forging or attempting to forge email messages.

Part D - Personal Use

(18) VU email accounts are provided for the purpose of academic and University related business operations. The University allows the reasonable use of email for personal use under the following conditions:

a. Personal use of email should not interfere with work responsibilities.

b. Personal use of email does not interfere with performance of University network services.
c. Personal emails must adhere to the IT Appropriate Use Policy and associated procedures.
d. Must not be used to run a private business whether for profit or not for-profit.

(19) The forwarding of nuisance emails such as chain letters, junk mail, jokes and frivolous attachments is strongly discouraged.

(20) Forwarding University emails to personal email accounts, where permitted, is subject to delivery issues and should be avoided.

Part E - Email Spam and Phishing

(21) Employees, students and other authorised users of VU's email service should make themselves aware of educational activities and resources provided by the University to help to identify potential cybersecurity threats and how to prevent them.

(22) An external email tag is inserted at the top of all emails that are sent to a VU employee email account from an email account outside of VU.

(23) Emails received that contain suspicious content, unexpected attachments or web links should not be opened and should be reported using the Report email button within Microsoft Outlook.

(24) The University will never ask for account details or passwords in an email or ask users to validate their password through email links (phishing).

(25) Sharing passwords with others is prohibited and individual users may be held responsible for all actions including any infringement carried out by a third party given access to their accounts.

(26) Employees or students who believe they may have responded to a phishing email must immediately phone ITS Service Desk on +61 3 9919 2777 (option 1).

(27) Sending or forwarding a phishing email or an attachment or link that contains a virus is prohibited. Employee and students at VU undertaking research or awareness campaigns may send emails containing such materials provided that it demonstrably refers to their area of research and is done so in a responsible manner and in accordance with any legislative requirements.

(28) The sending of unauthorised and unsolicited global or commercial email transmissions (spam) is not allowed. Mass electronic communications should only be sent in accordance with the IT Appropriate Use - Internal Mailing Lists Procedure.

Part F - Confidential and Restricted Emails

(29) Emails containing confidential or restricted information or attachments must be classified appropriately according to the Information and Asset Classification Framework.

(30) When sending or forwarding emails containing information or attachments classified as confidential or restricted to external organisations, the email should be signed and encrypted using an approved encryption method. These can include Microsoft Office password protect, and the encryption feature in WinZip. Passwords should be provided to the recipient using another form of communication such as phone or text message.

Part G - Monitoring and Audits

(31) Emails may be monitored for the operational integrity of the University Infrastructure and/or to comply with legal or regulatory requirements. See the Information Security Policy.

(32) VU has the right to access and conduct audits on emails sent and received from University email accounts as well as email records retained in University archive systems as part of the Information Security Policy and Information Security - IT Security Audit Authorities Procedure.

(33) If there is evidence that a student or employee is not adhering to University policies or procedures, the University reserves the right to take disciplinary action, including termination of access to University systems and services and/or legal action.

Part H - Retention of Emails

(34) All email records from University email accounts will be retained for ten (10) years. All of the Vice-Chancellor's email records will be retained indefinitely.

(35) Any exemption to the email retention period must be approved by the Chief Digital Officer and Executive Director Campus Services and Manager, Records and Archives Services.

Section 5 - HESF/ASQA/ESOS Alignment

(36) HESF: Standard 2.1 Facilities and Infrastructure, 7.3 Information Management.

(37) Outcome Standards for NVR Registered Training Organisations 2025: Standard 1.8 Facilities, Equipment and Resources.

Section 6 - Definitions

(38) Nil.

Section 7 - Supporting Documents and Information

(39) Online Safety and Security

(40) Information and Asset Classification Framework

(41) Best Practice Email Guidelines

Status and Details

Status	Current
Effective Date	12th August 2021
Review Date	15th March 2026
Approval Authority	Vice-Chancellor
Approval Date	12th August 2021
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services +61 3 9919 5576
Enquiries Contact	Rebecca Xuereb Senior Project and Administration Officer rebecca.xuereb@vu.edu.au