IT Appropriate Use Policy

Section 1 - Summary

(1) The purpose of this Policy is to provide a framework for the appropriate use of Information and Communication Technology IT Facilities and Services provided by Victoria University (VU).

(2) This Policy aims to inform staff, students, contractors, visitors and other authorised users of their obligations, restrictions and responsibilities when utilising ICT facilities and services and to protect vital ICT assets and minimise the risk of disruption to teaching, research and University business.

Section 2 - Accountability

Accountable/Responsible Officer	Role
Accountable Officer	Vice-President, Resources and Risk
Responsible Officer	Executive Director, IT Services

Key Decision-making powers under the Policy (if applicable)

(Delegated) Power	Role
n/a	

Section 3 - Scope / Application

(3) This Policy applies to:

a. All VU staff, students, contractors, visitors and other authorised users of IT Facilities and Services.
b. All authorised users connecting to ICT services from either personal (BYOD) or VU owned facilities.
c. IT Facilities and Services including but not limited to computer equipment, software, operating systems, storage media, communication facilities and accessories (voice, video and data), network accounts, network services, email accounts and central archive, web browsing, mobile phones and hand held devices.
d. ICT equipment and physical infrastructure located in communications rooms, data centres, work spaces, PC laboratories and other locations both within and outside of the University.

Section 4 - Definitions

(4) IT Facilities and Services

Section 5 - Policy Statement

(5) All VU staff, students, contractors, visitors and other authorised users of VU ICT facilities and services are expected to use these facilities and services in an appropriate and responsible manner.

(6) It is the responsibility of authorised users of IT Facilities and Services to make themselves aware of VU policies, procedures and guidelines related to information technology and conduct their activities accordingly.

(7) Users may be exempt from aspects of this policy where it is required for their role, studies or research and written permission from the head of the relevant organisational unit and the Executive Director, IT Services has been obtained.

Part A - Provision of ICT

(8) IT Facilities and Services are provided for the purpose of academic and University related business.

(9) The procurement and support of ICT software and hardware including PC's and laptop/tablets, desktop phones, mobile and hand held devices must comply with the ICT Software and Hardware policy.

(10) All reasonable precautions are to be taken for the safety, protection and appropriate use of VU IT Facilities and Services. Users are required to follow the Information Security Policy and associated procedures while utilising IT Facilities and Services in order to minimise risk to the University.

Part B - Personal Use

(11) VU IT Facilities and Services are provided for legitimate University business and operations; however, a small amount of personal use is permitted.

(12) Authorised users of VU IT Facilities and Services are responsible for exercising good judgement regarding reasonable personal use with guidance from Teaching staff and Student Services for students; and individual departmental managers and Directors/Deans for staff and other users.

(13) Costs incurred by the University through excessive personal use may be recovered directly from the individual concerned, and may lead to further disciplinary/legal actions.

Part C - Monitoring and Auditing

(14) All data created on corporate systems, including the communications infrastructure and desktop computers remains the property of VU. This includes emails sent and received from University staff and student email accounts as well as email retained in central archive.

(15) In order to protect the University's network, servers and data and/or to comply with legal or regulatory requirements, VU has the right to intercept, interrogate, or otherwise capture data created or received by individual users of IT Facilities and Services in accordance with the Information Security - IT Security Audit Authorities Procedure.

Part D - Unacceptable Use

(16) Under no circumstances are VU owned or managed resources to be used to engage in any activity that is illegal under state, federal or international law. Staff are expected to comply with the Appropriate Workplace Behaviour Policy at all times while utilising VU IT Facilities and Services and/or while connected to VU IT Facilities and Services.

(17) VU IT Facilities and Services must not be used by staff and students for the purpose of creating, accessing or transmitting or otherwise dealing with content which may reasonably be regarded as objectionable, obscene or offensive, or in a manner which is contrary to other University policies or which may otherwise expose the University to legal liability.

(18) Any person utilising VU IT Facilities and Services, must do so in accordance with the VU Copyright Policy and Intellectual Property Regulations. This includes, but is not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University.

(19) The use of VU IT Facilities and Services for unauthorised commercial or private gain is strictly prohibited. Use may be considered and approved by line managers in accordance with the Appropriate Workplace Behaviour Policy.

Part E - Access to ICT facilities and services

(20) Access to IT Facilities and Services must comply with the Information Security Policy and associated procedures unless otherwise exempt by other University policies. Authorised users of IT Facilities and Services will be held responsible for all actions including any infringement carried out by a third party given access to their accounts.

(21) University members are expected to comply with any local rules governing the use of shared IT resource spaces such as PC laboratories or laptop docking areas. Rules specific to PC laboratories can be found on signs located within the room and must be adhered to when using these spaces.

Part F - Collaboration Services

(22) Users of the University email and other collaboration services are prohibited from engaging in any activity that is illegal under state, federal or international law or against any University policy when using these services.

(23) Users of collaboration services must ensure all legislation and policies are strictly followed as well as adhere to the VU Policies and Procedures. In particular, the Discrimination and Harassment Prevention and Management Policy, Bullying Prevention and Management Policy, Sexual Harassment Response Policy, Appropriate Workplace Behaviour Policy, Equity and Diversity Plans and Strategies and the Student Charter Policy must be adhered to when utilising collaboration services.

(24) 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.

(25) The IT Appropriate Use - Email Procedure should be followed for all emails sent from University email accounts.

(26) All email records from University email accounts that have been moved to the central archive will be retained for ten (10) years. All of the Vice-Chacellor’s email records will be retained indefinitely.

(27) The use of collaboration services to send unauthorised and unsolicited global or commercial email messages (spam or junk mail) is strictly prohibited. Mass electronic communications should only be sent in accordance with the VU IT Appropriate Use - Internal Mailing Lists Procedure.

(28) Where facilities exist for a staff member to upload and display a profile image to a VU ICT service, the image must be consistent with representing the University and must not breach any aspect of VU’s Policies and Procedure.

Part G - Mobile, smartphone and handheld devices

(29) Members of the University allocated a mobile phone or hand held device are responsible for its proper use, care, maintenance and safekeeping. Negligence in this matter may result in the recovery of costs from the individual member concerned.

(30) Costs and charges for equipment and traffic (voice and data) incurred on VU mobile phones and hand held devices will be borne by the nominated cost centre. The University will cover the costs of all relevant University business related voice and data charges as well as charges related to limited personal use of VU mobile phones and hand held devices.

(31) Where personal voice and data charges incurred exceed the personal use limit set by the individual cost centre or the VU recommended limit, these costs are to be reimbursed by the staff member in accordance with the IT Appropriate Use - Mobile Phone Usage Reimbursement Procedure.

(32) VU staff travelling on official University business are permitted to use their University allocated mobile phone for making personal calls to home if approved by their department and provided that such calls are made as brief as possible.

(33) Costs incurred as the result of excessive personal use of VU mobile phones and hand held devices (voice and data) while overseas are to be reimbursed by the staff member in accordance with the IT Appropriate Use - Mobile Phone Usage Reimbursement Procedure.

(34) Where individual contracts of employment allow personal use of mobile phones or hand held devices, this will take precedence over this policy, however employees must strictly comply with the conditions of employment and the Appropriate Workplace Behaviour Policy when using their VU mobile phone.

Part H - Computers and IT Equipment

(35) Desktop and laptop computers must not be the sole repository of corporate, teaching or research data. All such data must be stored on University network drives or relevant VU systems, and new work backed up as soon as possible.

(36) Unauthorised tampering with any part of ICT infrastructure is strictly prohibited. Configuration changes to ICT facilities and physical infrastructure can only be performed by ITS and their authorised officers.

(37) Damage or alteration, either willfully or through negligence, of any hardware, software, physical plan, or communications component is strictly prohibited without proper authorisation from ITS.

(38) VU owned and leased ICT equipment must not be tampered with, defaced or permanently marked in any way. This includes removing or swapping items or components of ICT equipment with another item or component of ICT equipment without prior approval from ITS.

Part I - Network and Internet

(39) Deliberate modifications to the current production network are prohibited without proper authorisation.

(40) Deliberate introduction of malicious programs into the network or server (eg. Viruses, worms, Trojan horses, e-mail bombs, etc) is strictly prohibited.

(41) Deliberately effecting security breaches or disruptions of network communication is prohibited. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these activities are within the scope of regular duties.

(42) Port scanning or security scanning including the execution of any form of network monitoring is prohibited unless prior approval has been granted by ITS.

(43) Circumventing user authentication or security of any host, network or account is prohibited without proper

authorisation.

(44) Interfering with or denying service to any authorised user (eg. denial of service attack) is prohibited without proper authorisation.

(45) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, any authorised user's terminal session, via any means, locally or via the external Web is prohibited. This applies to sessions anywhere on the Web (i.e. including hacking sessions on external Web addresses).

(46) Any devices (including desktops and laptops) connected to the University network, whether owned by the staff member or the University, must have the current operating system patches applied to them and be equipped with the latest antivirus software, either by automated download or manual update.

(47) Access to the internet through Australia's academic and research network, AARNET, and is bound by AARNET's Access Policy (https://www.aarnet.edu.au/about-us/policies)

Part J - Security and Proprietary Information

(48) Authorised users should never provide confidential information over the Internet in response to unsolicited inquiries. Legitimate organisations like banks will never send such an unsolicited email request. Users should be wary of clicking on Web sites embedded in emails as this may redirect them to a malicious site. If ITS identifies an account as being compromised it will be locked out immediately and inform the account owner.

(49) Providing information about or lists of University staff and students to parties outside of VU is expressly forbidden unless it is part of normal job duties.

(50) Staff are responsible for considering the sensitivity of any information or data transmitted across the internal and external network, and ensuring that it is treated appropriately according to the policies of the University including the Privacy Policy. Examples of confidential information include but are not limited to:

a. examination results
b. confidential senior management communications
c. specifications of commercialised University developments or patents
d. vendor lists
e. details of commercial contracts and agreements, and
f. research data restricted by privacy and ethical concerns.

(51) Staff should take all necessary steps to prevent unauthorised access to confidential information and use secure modes of communication.

(52) Sensitive information held on desktops or transmitted across the Internet should be encrypted and sent over a secure network connection. Because information contained on laptop computers is especially vulnerable, additional special care should be exercised.

(53) Making fraudulent or unapproved offers of products, items, or services originating from any University ICT facility or service is prohibited (e.g. offering access to University services for personal benefit).

(54) Making statements about warranty, guarantees, or similar binding commitments on behalf of VU, expressly or implied, is prohibited unless it is a part of normal job duties.

Part K - Breaches of the policy

(55) All reported breaches of this Policy will be treated seriously and in accordance with the relevant Procedures.

(56) The consequences for substantiated breaches of this policy will depend on the seriousness of the case. Outcomes may include, but are not restricted to the following:

a. Disciplinary action in accordance with the relevant industrial instrument (for staff) or Student Misconduct Regulations 2019 (for students).
b. Withdrawal of access to the University email system and computer network.
c. Other users such as consultants and associates, who violate this policy, will be subject to appropriate action.

Section 6 - Procedures

(57) IT Appropriate Use - Internal Mailing Lists Procedure

(58) IT Appropriate Use - Mobile Phone Usage Reimbursement Procedure

Section 7 - Guidelines

(59) IT Appropriate Use - Email Procedure

Status and Details

Status	Historic
Effective Date	24th May 2018
Review Date	24th May 2021
Approval Authority	Vice-Chancellor
Approval Date	11th May 2018
Expiry Date	11th August 2021
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 9919 5576
Enquiries Contact	Jessica Carter Coordinator Quality Assurance +61 3 99196292

Glossary Terms and Definitions

"IT Facilities and Services" - Including but not limited to computer labs, equipment, software, operating systems, business systems and applications, data storage, communication facilities and accessories (voice, video and data), network accounts, network services, email accounts and central archive, web browsing, mobile phones and hand held devices.