IT Appropriate Use Policy

Section 1 - Summary

(1) The purpose of this Policy is to provide a framework for the appropriate use of Information Technology (IT) computing facilities and services provided to authorised users by Victoria University (VU).

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

Section 2 - HESF/ASQA/ESOS Alignment

(3) HESF: Standard 7.3 Information Management

Section 3 - Scope

(4) This Policy applies to:

a. All VU employees, students, visitors, contractors and third-party service providers both onshore and offshore or connecting to IT computing facilities, systems, networks and accounts, either on University premises or remotely.
b. All information assets that are owned and/or operated by VU and/or registered in any Domain Name System (DNS) domain owned by VU.
c. IT equipment and devices that are present on the University premises, but may not be owned or operated by the University.
d. Information assets outsourced or hosted at external/third-party service providers, if that asset resides in a VU domain or appears to be owned by VU.

Section 4 - Definitions

(5) IT Facilities and Services

(6) User – VU employees, students, contractors, visitors and third-party providers using IT computing facilities, systems, networks and accounts.

(7) Information Asset – Any information that is of value to the organisation. This term also includes the underlying supporting infrastructure such as business processes, hardware, networks, storage, applications, third-party providers and storage amongst others.

Section 5 - Policy Statement

(8) All employees, students, contractors, visitors and other users of IT facilities and services are expected to use these facilities and services in an appropriate and responsible manner.

(9) It is the responsibility of employees, students, contractors and visitors to make themselves aware of VU policies, procedures and guidelines related to Information Technology Services and conduct their activities accordingly.

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

(11) The use of IT facilities and services must comply with this Policy, the Information Security Policy, the Information Security - User Access Management Procedure, IT Security Standards and other relevant University rules, policies and procedures, including the:

a. Appropriate Workplace Behaviour Policy and Student Charter Policy; and
b. Bullying Prevention and Management Policy, Sexual Assault Response Policy, Sexual Harassment Response Policy, and the Discrimination and Harassment Prevention and Management Policy; and
c. Privacy Policy, Copyright Policy and Intellectual Property Regulations 2013.

Part A - Provision and Use of IT

(12) The procurement and support of IT software and hardware including computers, laptops, desktop phones, mobile and hand-held devices must comply with the IT Hardware and Software Policy.

(13) Access to IT facilities and services must comply with the Information Security Policy, Information Security - User Access Management Procedure and other associated procedures and IT Security Standards unless otherwise exempt by other University policies.

(14) Users must take all reasonable precautions for the safety and protection of VU data and information assets from unauthorised access or disclosure in order to minimise risk to the University by adhering to the handling requirements and security controls based on its classification and the policies of the University, including the Information Security Policy and the Privacy Policy.

(15) Desktop and laptop computers must not be the sole repository of corporate, teaching or research data. Corporate, teaching or research data should be stored on University approved storage and protected based on their classification and sensitivity in accordance with the Information Security Policy.

(16) Users are responsible for the protection of their individual account and password and must not share passwords with anyone or allow others to use their account. Users will be held responsible for all actions including any infringement carried out by a third-party given access to their accounts.

(17) Computers and devices connecting to or accessing IT systems and services should implement session and screen locking mechanisms to prevent unauthorised access to the user’s account or University data and information.

(18) All computers and devices connected to the University network including computers and devices not owned or managed by 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.

(19) Physical security measures and controls are to be used to protect computer systems, personnel, and data and communications systems located in secure locations. Access to such areas must be restricted to those who have an approved need to be there.

(20) University members are expected to comply with any local rules governing the use of shared IT resource spaces such as computer laboratories or laptop docking areas.

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

(22) Personal profile images uploaded to VU systems must be appropriate and consistent with representing the University. Employees should follow the Staff Profile Image Guidelines.

(23) 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.

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

Personal Use

(25) IT facilities and services are provided for the purpose of academic and University related business operations. All employees, students, contractors and visitors are to use these facilities and services for their authorised and intended purpose, however, a small amount of personal use is permitted.

(26) Users are responsible for exercising good judgement regarding reasonable personal use in line with their duties and responsibilities with guidance from Teaching staff and Student Services for students; and individual departmental managers and Directors/Deans for employees and other users.

(27) 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.

(28) Mobile phone costs incurred that exceed the personal use limit set by the individual cost centre or the VU recommended limit, are to be reimbursed by the employee in accordance with the IT Appropriate Use - Mobile Phone Usage Reimbursement Procedure.

(29) VU employees 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.

(30) 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.

Unacceptable Use

(31) The following is inappropriate and prohibited when accessing, connecting to or using IT facilities and services:

a. Engaging in any activity that is illegal under State, Federal or international law or in breach of any University policy.
b. Use for the purpose of creating, accessing or transmitting or otherwise dealing with content which is 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.
c. Use that violates the VU Copyright Policy and Intellectual Property Regulations 2013 including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University.
d. Use for commercial or private gain unless approved by a line manager in accordance with the Appropriate

Workplace Behaviour Policy.

e. Sending of unauthorised and unsolicited global or commercial messages (spam or junk mail).
f. Unauthorised tampering with any part of IT infrastructure or deliberate modification to the current production network. Configuration changes can only be performed by Information Technology Services (ITS) and authorised officers.
g. Damage or alteration, either willfully or through negligence, of any hardware, software, physical plan, or communications component without proper authorisation from ITS.
h. Tamper with, deface or permanently mark VU owned or leased IT equipment in any way. This includes removing or swapping items or components of IT equipment with another item or component of IT equipment without prior approval from ITS.
i. Deliberate introduction of malicious programs into the University network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc).
j. Deliberately effecting security breaches or disruptions of University network or business systems including, 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.
k. Port scanning or security scanning including the execution of any form of network monitoring without prior approval from ITS.
l. Circumventing user authentication or security of any host, network or account without proper authorisation.
m. Interfering with or denying service to any authorised user (e.g. denial of service attack).
n. 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. This applies to sessions anywhere on the Web (i.e. including hacking sessions on external Web addresses).
o. Making fraudulent or unapproved offers of products, items, or services originating from any University IT facility or service is prohibited (e.g. offering access to University services for personal benefit).
p. 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.
q. Providing information about or lists of University employees and students to parties outside of VU is expressly forbidden unless it is part of normal job duties.

Monitoring and Auditing

(32) All information and data created on University IT systems, including communications systems, computers and devices remains the property of VU. This includes but is not limited to emails sent and received from University employee and student email accounts, emails retained in central archive, voicemail, text messages and instant messages.

(33) 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, search, inspect, review, 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.

Breaches of the Policy

(34) All breaches of this Policy will be treated seriously.

(35) The outcome of a substantiated breach of this Policy may include, is not limited to the following:

a. Disciplinary action in accordance with the relevant enterprise agreement (for employees) or Student Misconduct Regulations 2019 (for students).

b. Withdrawal of access to the University email service, system access and/or network services.
c. Other users such as consultants and associates, who breach this Policy, will be subject to appropriate action including but not limited to the outcomes available under clause (35)b of this Policy.

Section 6 - Procedures

(36) IT Appropriate Use - Internal Mailing Lists Procedure

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

(38) IT Appropriate Use - Email Procedure

Section 7 - Supporting Documents and Information

(39) Information and Asset Classification Framework

(40) IT Security Standards

(41) Staff Profile Image Guidelines

Status and Details

Status	Current
Effective Date	12th August 2021
Review Date	12th August 2024
Approval Authority	Vice-Chancellor
Approval Date	12th August 2021
Expiry Date	Not Applicable
Accountable Officer	Richard Constantine Vice-President, Resources and Risk +61 3 99194753
Responsible Officer	Zoran Sugarevski Executive Director, IT Services +61 3 99195076
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.