IS Acceptable Use Policy

Section 1 - Key Information

Policy Type and Approval Body	Administrative – Vice-Chancellor
Accountable Executive – Policy	Chief Operating Officer
Responsible Manager – Policy	Chief Information Officer
Review Date	26 February 2028

Section 2 - Purpose

(1) This Policy sets out the conditions and requirements applicable to the use of La Trobe University (University) IS Assets and Services.

(2) The Policy aims to ensure the University's IS Assets and Services are used in a manner consistent with the University's values and legal requirements. It is designed to mitigate risks of service disruption and data breaches caused by cyberattacks and unauthorised or unintentional actions.

Section 3 - Scope

(3) This Policy applies to all current and past:

a. staff;
b. students;
c. adjunct, emeritus and honorary appointees;
d. any other software accounts that are provisioned by the University; and
e. other members of the University who are given access to University IS assets and services.

(4) This Policy also applies to all Users and uses of the University's IS resources, regardless of whether a device used is a University IS resource or a personally owned device. Such resources can include:

a. University internet via WiFi and LAN;
b. applications which are licensed by the University including cloud-based services; or
c. online accounts such as social media which are used to represent the University.

Section 4 - Key Decisions

Key Decisions	Role
Investigate a User's La Trobe account or use of IS resources.	Chief Information Officer (CIO)
Approve access to a User's account or the provision of information from a User's account.	Chief Information Officer (CIO)

Section 5 - Policy Statement

Conditions and requirements of use

(5) Only approved Users can use University IS Assets.

(6) The University will approve access to IS Assets in accordance with the access requirements set by the relevant IS resource owner, such as email systems.

(7) Access to IS Assets will be provided following the 'Principle of Least Privilege.' Users will be given only the minimum privileges and access rights necessary for their role.

(8) Users must only use University IS Assets for authorised purposes, which include:

a. carrying out duties of their role/position for or on behalf of the University;
b. engaging in study, research, and collaborative learning; and
c. limited, non-commercial acceptable personal use.

(9) The University accepts no responsibility for loss or damage (including loss of data) or consequential loss or damage arising from the use or maintenance of its IS Assets.

(10) Users must take responsibility for using University IS Assets in an ethical, respectful, compliant, secure and legal manner. At all times, Users must:

a. not share passwords and other login credentials;
b. report suspicious activity or any breach of policy relating to ICT use;
c. complete and adhere to all training provided on IT security awareness;
d. be aware and alert to risks relating to email phishing and other tactics used in cyber attacks;
e. only use software or applications that have been authorised for use within the University IS environment;
f. comply with all University policies, procedures, and directives regarding IS Assets and Information Assets, including:
    i. this IS Acceptable Use Policy;
    ii. Information Security Policy
    iii. Asset Management Policy
    iv. Desktop Equipment Policy
    v. Mobile Communication Device Policy
    vi. Privacy Policy
    vii. Records Management Policy
    viii. Procurement Policy
g. comply with any conditions or terms of use imposed by suppliers as part of license terms;
h. conduct themselves in a manner consistent with the requirements of all relevant University conduct policies, including, but not limited to the:
    i. Code of Conduct
    ii. Student Behaviours Policy
    iii. Sexual Harm Prevention and Response Policy
i. not use IS Assets to undermine academic integrity;
j. refrain from accessing, disseminating, or downloading prohibited content; and
k. act in a lawful manner, including with regard to intellectual property and copyright law.

(11) Users are responsible for activity initiated from their University account. Therefore, Users must only access University IS Assets using their own account and take reasonable steps to protect their account(s) and IS Assets from unauthorised access/use.

(12) Information stored on IS Assets remains the sole property of the University.

(13) The University reserves the right to:

a. carry out security audits on IS Assets;
b. investigate any use of IS Assets, block, copy, delete, or take possession of IS Assets where there is suspicion of a policy violation or unlawful action, or to protect or recover the University's IS;
c. inspect, copy, and disclose documents and information stored on University IS resources to third parties to comply with legal processes (e.g., Freedom of Information Act requests, subpoenas) and efficiently manage University affairs;
d. block or restrict access to specific sites, email addresses, applications, and other digital resources deemed a risk to the University, its staff, and students; and
e. monitor online activity, including internet browsing, emails, and file transfers, for risk management and audit purposes.

(14) Only the Chief Information Officer (CIO) or their nominee may authorise the investigation/monitoring of a user's account for suspected misuse.

(15) A breach of this Policy may result in disciplinary action (e.g., termination of engagement/appointment) and, in severe cases, referral to public agencies.

Section 6 - Procedures

User approval

(16) Procedures detail the mandatory process, actions and the "how to" applicable to the Policy subject matter.

(17) Information Services will facilitate an individual being given an LTU account where approval has been granted as follows:

a. Staff – [via Onboarding process]
b. Students – [via Enrolment process]
c. Contractors/consultants – [Head of School/Dept]
d. Honourees and visiting fellows – [Dean of School]

(18) The approval process for IS resources, applications or platforms will be determined by the system owner in line with policy principles.

Acceptable use

General

(19) The University provides IS resources to enable staff, students, and other University members (including Council members, contractors, volunteers, and honorary appointees) to fulfil their roles, engage in learning and collaboration activities, and participate in the broader research and learning community.

(20) Users must use IS Assets responsibly, respectfully, as intended, and in line with this Policy. Expected uses include

but are not limited to:

a. using messaging technologies, including email, for work or study-related communication;
b. using standard software provided by the University for work or study tasks;
c. accessing and using online resources via the Internet; or
d. engaging in limited personal use (see below).

(21) Users must exercise reasonable care, including:

a. using caution when opening links and reporting suspicious links to Information Services;
b. reporting unusual system behaviour to IS Service Desk;
c. using unique, strong passwords and keeping them secure;
d. not allowing others to use their login details;
e. complying with Multi-Factor Authentication requirements;
f. screen-locking unattended devices; and
g. reporting theft or loss of IS Assets to Information Services.

Email

(22) The privacy, confidentiality, and integrity of email cannot be guaranteed by La Trobe.

(23) Broadcast emails must be reviewed and approved per the Student Communications Policy and other relevant policies.

(24) Personal and non-La Trobe email accounts must not be used for University-related activities or storing University Information Assets.

(25) Staff must not use their La Trobe email for personal purposes or provide it as contact information for personal matters.

Data Storage and File Sharing

(26) The University permits limited non-commercial, acceptable personal use of IS resources, including:

a. reading news or entertainment content during breaks;
b. conducting personal administration tasks (e.g., bookings, banking);
c. limited personal correspondence via personal messaging platforms; and
d. attending to a carer or other responsibilities.

(27) Unacceptable personal use is outlined under the Unacceptable Use section.

Personal Devices

(28) The University acknowledges that some Users use personal devices (e.g., phones, laptops, tablets) to access University IS resources.

(29) When accessing IS Assets or University Information Assets with personal devices, Users must ensure appropriate security controls, including:

a. complying with all LTU IT Security measures including MFA and password management;
b. installing and maintaining security software, including anti-malware and firewalls, and using remote wiping software if available; and

c. not reusing passwords for personal accounts for any LTU related activity.

(30) Users must not store University Information Assets on personal devices.

Unacceptable Use

(31) Users must not:

a. engage in any illegal activity under State or Commonwealth law or University policy;
b. create, access, transmit, or deal with objectionable or obscene content;
c. expose the University to legal liability, including copyright and intellectual property infringement;
d. use personal email addresses for work correspondence or work email addresses for personal affairs;
e. send unsolicited messages (spam);
f. make unauthorised offers of products or services;
g. make unauthorised binding commitments on behalf of the University;
h. disclose personal information without consent or legal permission; and
i. share or disclose University Information Assets inappropriately.

(32) Unacceptable personal use includes:

a. any use violating the law or University policy;
b. use interfering with work duties;
c. use disrupting others' ability to work or study (e.g., audible sound files in shared areas);
d. use supporting a personal commercial enterprise;
e. using LTU email for personal matters (e.g., banking);
f. storing personal items on LTU devices or network or cloud storage locations;
g. use personal or commercial VPN services on LTU devices; and
h. use high-risk file transfer services such as bit torrents on LTU devices.

Access and Monitoring

(33) Upon request, the CIO or CISO may authorise:

a. access or monitoring of a User's account;
b. copying and producing information required for legal processes; and
c. providing account access in cases such as unplanned absences.

(34) Requests should be directed to the CISO via a request in AskIS.

(35) Authorised Information Services staff may monitor and analyse IS Assets for efficiency, security, and effectiveness.

(36) Information Services staff must only access user accounts with consent or per this Policy.

(37) The Chief Information Security Officer (CISO) or the LTU Security Team may contact users directly to determine the source of or request the immediate halt of any activity considered high risk or in conflict with this Policy.

(38) Access to any or all IS services may be suspended without notice for a user or group of users if security monitoring determines the high likelihood of a compromise or severe breach of this policy.

Section 7 - Definitions

(39) For the purpose of this policy and procedure:

a. Acceptable Personal Use: limited, non-commercial use of University ICT resources by Users for personal activities, provided it does not interfere with their professional responsibilities or the performance of University systems.
b. Antimalware Software: software designed to detect, prevent, and remove malicious software (malware) from IS resources.
c. Authorised Purpose: activities related to carrying out the duties of a person's role/position for or on behalf of the University, engaging in study, research, and collaborative learning, and limited, non-commercial acceptable personal use.
d. Cyberattack: any attempt to expose, alter, disable, destroy, steal, or gain unauthorised access to or make unauthorised use of a computer system, network, or device
e. Data Breach: an incident involving the unauthorised access, disclosure, or loss of sensitive, protected, or confidential information, often resulting in data being exposed to individuals who are not authorised to view it.
f. Data Custodian: the individual or entity responsible for the management and protection of specific data within the University, ensuring it is handled in accordance with relevant policies and legal requirements.
g. Email: a method of exchanging digital messages over the internet, allowing Users to communicate within and outside the University. University email accounts are to be used solely for University-related activities.
h. Encryption: the process of converting data into a code to prevent unauthorised access, ensuring the data is only accessible to those with the decryption key or password.
i. Firewall: a network security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules, establishing a barrier between a trusted internal network and untrusted external networks.
j. Freedom of Information Act: an Australian law giving the public the right to access documents from the Government of the Commonwealth of Australia and its agencies, including public universities, subject to certain exemptions.
k. IS Assets: all information and communication technology resources and systems, including but not limited to computers (desktops and laptops), mobile devices, software, networks, databases, cloud repositories, and electronic communication systems owned or operated by La Trobe University.
l. Information Assets: Any knowledge, data, or information (irrespective of format) that has value to the University and consequently needs to be suitably protected.
m. Intellectual Property: Creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce, which are protected by law to give the creator exclusive rights to use them.
n. malware: malicious software designed to harm, exploit, or otherwise compromise the operation of IS resources. Examples include viruses, worms, Trojan horses, ransomware, spyware, and adware.
o. Multi-Factor Authentication (MFA): A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
p. Personal Device: any device not owned or provided by the University, including but not limited to personal computers, laptops, tablets, smartphones, and external storage devices, used to access University IS resources.
q. Principle of Least Privilege: a security concept wherein users are granted the minimum levels of access – or permissions – needed to perform their job functions.
r. Prohibited Content: material the creation, publication, transmission, display, making available, sale, or possession of which is prohibited or restricted under any law of the Commonwealth or Victorian Parliament. This includes but is not limited to offensive, obscene, or illegal content.

s. Records Management Policy: a University policy outlining the principles, responsibilities, and requirements for the systematic control of records throughout their lifecycle, from creation and receipt through to disposal or permanent preservation.
t. Remote Wiping: the ability to remotely erase data from a device to protect sensitive information in case the device is lost, stolen, or compromised.
u. Spam: unsolicited, often irrelevant or inappropriate messages sent over the internet to a large number of users, typically for the purposes of advertising, phishing, spreading malware, or other malicious activiti
v. User/Users: any authorised individual who uses the University's IS resources. This includes staff, students, honorary appointees, Council members, contractors, volunteers, and any other person granted access to University IS resources

Section 8 - Authority and Associated Information

(40) This Policy is made under the La Trobe University Act 2009.

(41) Associated information includes:

a. Information Security Policy
b. Asset Management Policy

Status and Details

Status	Current
Effective Date	26th February 2025
Review Date	26th February 2028
Approval Authority	Vice-Chancellor
Approval Date	26th February 2025
Expiry Date	Not Applicable
Responsible Manager - Policy	Shainal Kavar Chief Information Officer
Author	David Willett Chief Information Security Officer
Enquiries Contact	Information Services 03) 9479 1500