POLICIES AND PROCEDURES

LINCOLN UNIVERSITY
TE WHARE WĀNAKA O AORAKI

IT Acceptable Use Policy

Last Modified:	30 January 2023
Review Date:	31 January 2024
Business Owner:	Chief Operating Officer
Approval Authority:	Vice-Chancellor

1. Purpose

This Acceptable Use Policy establishes specific requirements for the appropriate use of all information technology (IT) resources at Lincoln University.

This policy should be interpreted broadly and in line with Lincoln University's values to include the use of new and developing technologies not explicitly listed in this policy. In general, acceptable use means respecting the rights of other users, the security and integrity of the physical and virtual resources and all relevant license and contractual agreements.

Some Faculties, departments or business units within the University may maintain additional IT systems. This policy also applies to such systems and their users.

2. Definitions

IT resources include but are not limited to:

- Wired, wireless, VPN-connected or other University provided networks, including personal devices connected to them;
- Network equipment including Internet of Things (IoT) devices;
- Cloud-based services and applications;
- Servers, PCs, portable computers and peripherals (e.g. laptops, notebooks, tablets and mobile / smart devices, printers, scanners, external drives and other portable media);
- Software and other services (including e-mail and the Internet) accessed through any of the above;
- Data and information assets accessed through any of the above (regardless of where they are located or how they are processed or communicated).

3. Outcomes

This policy seeks to:

- Define what constitutes acceptable use of Lincoln University IT resources and the obligations on those using the resources.
- Provide guidance on what constitutes unacceptable use of Lincoln University IT resources.
- Ensure the confidentiality, integrity, availability, reliability, security, and performance of information technology systems.
- Ensure the use of information technology systems is consistent with the principles and values that govern the use of other University services.

4. Policy

4.1 Acceptable Use of Lincoln University IT resources includes:

- Accessing and using IT systems and facilities for legitimate work and study purposes.
- Accessing and using Lincoln provided network resources by wholly owned subsidiaries and University tenants as agreed in tenancy agreements and subject to all relevant University policies including this policy.
- Accessing information from the Internet and using general Internet services (such as email) for legitimate work and study purposes.
- Undertaking activities that are otherwise deemed unacceptable if they have been explicitly authorised by University management.
- Using personal devices for legitimate work and study purposes when at home, travelling or in the office, if properly authorised.
- Accessing and using IT facilities for personal or recreational purposes, provided such use is incidental and reasonable, does not adversely affect other IT users and is not illegal. Such use is considered a privilege, not a right, and may be withdrawn at any time.

4.2 Unacceptable Use of Lincoln University IT resources includes, but is not limited to:

©This document is the property of Lincoln University. Once printed this document is an uncontrolled version. For the official, current version refer to the Lincoln University Policy Library.

- Interfering with the University in meeting its legal obligations.
- Connecting unauthorised or privately owned devices to University networks other than networks or other facilities provided for this purpose e.g. guest wifi and residential networks.
- Creating, viewing, saving or distributing material that could be considered offensive, obscene, indecent, illegal or reflect badly on the University.
- Deliberately creating, introducing or distributing computer viruses or other malicious software.
- Excessive use of University IT resources, such as storing non-University related files on University provided storage, or consuming excessive Internet bandwidth such as up/downloading large non-work related video files.
- Monitoring, probing for security vulnerabilities, intercepting, altering, hacking or attempting any unauthorised access to University systems, networks, data and facilities unless explicitly authorised by the Information Technology Services (ITS) Director.
- Improperly and inappropriately revealing, disclosing or sharing confidential personal or proprietary information through websites, blogs, discussion forums, email, social media etc.
- Pirating, plagiarizing, using, copying or distributing information in contravention of copyright or other laws.
- Annoying, harassing or defaming others, distributing spam, spreading malicious rumours and other antisocial behavior.
- Sharing or disclosing personal user identities, passwords, security tokens etc. with anyone else.
- Impersonating or making other inaccurate or false representations as to an identity or the identity of others.
- Storing confidential or sensitive University information on a BYOD device or non-University storage location unencrypted without prior approval.
- Using University IT facilities to work on behalf of other organisations, including charities and not-for-profit organisations, without prior approval from University management.

- Developing, planning, deployment, and management of Wireless network infrastructure without the approval and involvement of ITS.
- Changing IT-related staff, teaching and/or research equipment or resources without prior approval of IT. This includes the installation of unauthorised equipment, services or software.

4.3 User Obligations under this policy

To ensure the IT resources continue to be effective for teaching, learning, research and administration, all users are required to take adequate care of the equipment and facilities they use. Any faults, damage or incidents where service is compromised are to be reported to ITS at the earliest opportunity. Users must be respectful of the personal rights of others while using information technology resources. Users must commit themselves to comply with all of the University licensing, contractual and copyright obligations and laws of New Zealand as well as all other relevant University policies.

All users, regardless of their physical location or the devices they use, must maintain and follow safe security practices so as not to jeopardize the University's information technology resources in any way. Users should also be vigilant of cyber security threats and should take reasonable steps to protect themselves. Users should err on the side of caution and contact the IT Service Desk in the first instance for advice.

All users should consume Lincoln University information technology resources in a fair and equitable manner and minimise disruption to themselves and others by performing regular housekeeping. Housekeeping activities include but are not limited to:

- Maintaining good data management practices while prioritising the safety and security of University data.
- Storing work and research data in approved locations.

- Regularly restarting computers, or as otherwise advised.
- Keeping workspaces clean and considering placement of items so that the environment does not interfere or harm the computer equipment
- Regularly reviewing user access and permissions and notifying ITS so they can update access rights and ownership information for online/network resources and equipment.
- Properly disposing of IT devices or storage media if they contain, or may contain, personal or University information. Such information must be disposed of properly via the Service Desk.

4.4 Right to Monitor

Users are granted use of electronic information systems and network services and resources to conduct University business and undertake study and other authorised activities. ITS reserves and retains the right to access, inspect, monitor and audit all information technology resources covered by this policy.

4.5 Consequences of breaching the IT Acceptable Use Policy

Users who misuse any information technology resources and services may have their access suspended without notice. Staff who breach this Acceptable Use policy may be subject to investigation and disciplinary action in accordance with HR policies. Students who breach this policy may be subject to investigation and disciplinary action in accordance with the student discipline policies. Wholly owned subsidiaries and University tenants who breach this policy will be subject to network termination or reduction in offered services until the breach is remedied.

5. Responsibilities

5.1 The Vice-Chancellor has overall responsibility for ensuring information technology meets University requirements.

5.2 The IT Director has responsibility to provide fit-for-purpose IT services and support in an efficient manner.

5.3 Managerial staff are responsible for ensuring that individual staff, student, third parties and all other users consume information technology resources and services in line with this policy and in the best interests of the Lincoln University.

5.4 All staff, students, contractors, third parties, guests and users must inform Information Technology Services in the event of lost assets, damage or security incidents.

6. LINKS TO PROCEDURE(S) AND OTHER RESOURCES

This policy seeks to ensure compliance with relevant legislation which includes, but is not limited to:

Education and Training Act 2020

Crimes Act 1961

Harmful Digital Communications Act 2015

Privacy Act 2020

©This document is the property of Lincoln University. Once printed this document is an uncontrolled version. For the official, current version refer to the Lincoln University Policy Library.