Acceptable Use Policy

Category: General;
Jurisdiction: Provost and Vice President Academic; Vice President, Administration and Finance;
Approval Authority: Executive Team;
Established on: October 28, 2025;
Amendments: N/A;
Most Recent Review: N/A;

---

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to ensure that Lakehead University's IT Resources are used effectively, ethically, and securely to support the University's academic, research, and administrative missions. This policy aims to facilitate teaching, learning, and research while safeguarding IT infrastructure from threats and unauthorized access. This policy promotes adherence to applicable laws and regulations, ensures the integrity, confidentiality, and availability of data, and maintains reliable system operations and access. Additionally, the AUP encourages ethical and responsible use of IT Resources, supports educational and administrative activities, and enhances communication and collaboration within the University community. By adhering to these guidelines, we maintain a secure, lawful, and productive computing environment for all Users.

2. Scope

This Acceptable Use Policy (AUP) applies to all University Users and encompasses a wide range of IT Resources. However, this policy does not cover Third-Party Applications and

Services that are outside the University's control and responsibility, such as publisher sites, classroom response systems, and other external platforms.

This policy applies to IT Resources used in various locations, including on-campus IT infrastructure, remote access usage from off-campus locations, and University-owned or leased facilities outside the main campuses.

The usage contexts covered by this policy include scholarly purposes, such as classes, research, and academic projects; administrative activities, including management, record-keeping, and communication; and Personal Use under specific conditions.
By outlining these parameters, the AUP ensures that all Users understand their responsibilities when accessing and utilizing the University's IT Resources, both on and off-campus, for a variety of purposes.

3. Definitions

Account Managers: Account Managers oversee user accounts and access control within University IT Resources. This includes IT staff managing authentication systems and supervisors granting, reviewing, and revoking employee access. They ensure compliance with access policies, safeguard credentials, and maintain data security.

Compliance: Adherence to all applicable local, provincial, federal, and international laws and regulations, as well as University policies and guidelines.

Disciplinary Action: Measures taken by the University in response to violations of this policy, which can include warnings, suspension of access, academic sanctions, and termination of employment.

Intellectual Property: Creations of the mind, including inventions, literary and artistic works, designs, symbols, names, and images used in commerce. This also includes software, databases, and other content covered under licensing agreements.

Information Technology (IT) Resources: Includes all computing equipment (desktops, laptops, servers), mobile devices (smartphones, tablets), networking resources (Wi-Fi, wired networks, remote access services), software (both commercial and University-developed applications), digital storage (cloud services, internal data storage systems), communication

systems (email, messaging platforms, collaboration tools), and online platforms (learning management systems, library databases, administrative portals) provided or supported by the university.

Monitoring: The process of systematically observing and recording network and system usage to ensure Compliance with this policy, maintain system integrity, and prevent misuse.

Personal Use: Use of IT Resources for activities not directly related to the academic, research, or administrative functions of the University, which is permissible under certain conditions as specified in this policy.

Sensitive Data: Any kind of information protected against unwarranted disclosure.

System Administrators:
System Administrators are individuals responsible for the management, configuration, maintenance, and security of University IT Resources, including servers, networks, applications, and storage systems. They ensure system integrity, enforce security policies, manage software updates, and monitor IT infrastructure for performance, compliance, and security threats.

Third-Party Applications and Services: Applications, platforms, or services developed, owned, or operated by external entities that are not directly controlled or managed by the University. These may include software, cloud-based tools, or online services. Users are responsible for ensuring compliance with the terms of use and privacy policies of these services.

Unauthorized Access: Any access to IT Resources without proper authorization, including hacking, circumventing security measures, and accessing resources beyond granted permissions.

University: refers to Lakehead University.

Users: Refers to all members of the Lakehead University community, including students (undergraduate, graduate, part-time, and full-time), faculty (including adjuncts and visiting professors), staff (administrative, research, technical, etc.), contractors, consultants, alumni, emeriti, and guests and visitors, including participants in University-sponsored events who may use IT Resources.

4. Policy Statements

The following policy statements outline the acceptable and unacceptable uses of Lakehead University's IT Resources. These guidelines are designed to ensure that IT Resources are used effectively, ethically, and securely to support the University's missions. All Users are expected to adhere to these guidelines to maintain a secure and productive computing environment.

Proper Use:

Users must use IT Resources only for their intended purposes, which are related to the academic, research, and administrative functions of Lakehead University. All Users are expected to utilize these resources in a manner that supports the University's mission and objectives.

Prohibited Activities:

Engaging in the following activities is strictly prohibited:

- Unauthorized access to IT Resources, including hacking and circumventing security measures.
- Illegal downloading or distribution of copyrighted materials.
- Sending spam, phishing emails, or any form of fraudulent communication.
- Engaging in harassing, defamatory, or malicious behaviours that could harm individuals or the University's reputation.
- Using IT Resources for personal financial gain or commercial activities not sanctioned by the University.

Security and Privacy:

Users are expected to maintain the security and privacy of University IT Resources by:

- Following best practices for password creation and management.
- Not sharing accounts or login credentials with others.
- Respecting privacy laws and University confidentiality agreements.
- Ensuring that Sensitive Data is protected and not disclosed without authorization.

System Administrators and Account Managers have additional responsibilities to ensure the integrity and security of IT Resources. These responsibilities include:

- Account Provisioning and Deprovisioning: Ensuring that user accounts are created, modified, and removed in accordance with University policies, guidelines and user roles.
- Guidelines and Procedures development: The development of any necessary procedures or guidelines to maintain systems and accounts.
- Access Control: Implementing the principle of least privilege, ensuring users only have access to systems and data necessary for their role.
- Security Monitoring: Regularly reviewing logs and system activity for signs of unauthorized access, misuse, or anomalies.
- Incident Response: Promptly addressing security incidents, breaches, and policy violations in accordance with University procedures.
- Data Protection: Ensuring sensitive University data is encrypted in transit and at rest, where applicable, and implementing measures to prevent data loss.
- Tool and Software Adoption: Ensuring that any new IT tools, platforms, or services used within the University meet security, privacy, and Compliance requirements before deployment.
- Regular Audits and Updates: Conducting periodic security audits, patching vulnerabilities, and updating software and systems to maintain security compliance.

Monitoring and Compliance:

Lakehead University reserves the right to monitor network and system usage to ensure compliance with this policy, maintain system integrity, and prevent misuse. Users should be aware that their activities on University IT Resources may be monitored and reviewed for these purposes. Additional information can be found in the Electronic Monitoring Policy.

Resource Limits and Disruption:

Users must not engage in activities that could impair access for others, such as excessive use of network bandwidth, email storage, or printing facilities. IT Resources should be used in a manner that conserves resources and ensures fair access for all Users.

Personal Use:

Limited Personal Use of IT Resources is permitted, provided it does not interfere with University operations, the User's duties, or the rights of other Users. Personal Use must comply with all other aspects of this policy and not compromise the security or functionality of IT Resources.

Intellectual Property:

Users must respect Intellectual Property rights, including adherence to licensing agreements for software, databases, and other content. Unauthorized copying, use, or distribution of licensed software or copyrighted materials is prohibited.

Reporting Misuse:

Users are encouraged to promptly report any observed misuse of IT Resources or security breaches to the appropriate University authority, supervisor, or Technology Services Centre Helpdesk. Timely reporting helps the University to mitigate potential harm and ensures a secure computing environment.

Compliance with Laws and Regulations:

Users must comply with all applicable local, provincial, federal, and international laws and regulations in their use of IT Resources. This includes, but is not limited to, data protection regulations, copyright laws, and other relevant legal, ethical, and professional standards.

5. Enforcement and Administration

Lakehead University reserves the right to enforce the AUP and administer appropriate Disciplinary Actions for non-Compliance. The enforcement of this policy ensures that all Users adhere to the guidelines set forth to maintain a secure, lawful, and productive computing environment.

This section details the Disciplinary Actions or penalties for non-Compliance, which can range from temporary suspension of access to IT Resources to more severe academic or employment consequences. The consequences for violating this policy are designed to reflect the severity of the infraction and can include the following:

Disciplinary Action: This can include formal reprimands, probation, or other disciplinary measures under the relevant University code of conduct policies. For students, this may affect their standing within their academic program, while employees may face actions up to and including termination of employment. Disciplinary Actions are subject to appeal as per the applicable procedures outlined in the relevant policies.

Warnings: Minor or first-time violations may result in written or verbal warnings from University administrators. This is often the first step in addressing non-compliant behaviour.

Temporary Suspension of Access: Users may temporarily lose access to certain IT Resources while an investigation is conducted or as a penalty for non-Compliance. This can include suspending access to email accounts, the network, or specific software.

Permanent Revocation of Access: For more serious offenses, Users might permanently lose access to University IT Resources. This could affect their ability to perform academic or job-related duties effectively.

Restitution and Costs: If the violation involves damage to University property or resources, the responsible party may be required to pay for repairs, replacements, and the cost of labour to rectify the issue.

Academic Sanctions: Students may face specific academic sanctions, such as failure of assignments, failure of courses, or other penalties that can affect their academic record and progress (as per the Student Code of Conduct).

Appeals Process: Individuals subject to disciplinary actions under this policy have the right to appeal decisions through the processes outlined in applicable University policies, such as the Student Code of Conduct, Employee Code of Conduct, or other relevant University policies listed in the "Related Policies, Procedures, Guidelines" section of this document. Appeals should be submitted in accordance with the specific procedures detailed in the applicable policy.

Legal Action and Notification to External Bodies: In cases where laws have been broken, such as Unauthorized Access, theft of Intellectual Property, or distribution of illicit material, individuals may face criminal charges or civil actions. Additionally, for violations involving professional misconduct or legal issues, the University may be required to notify professional licensing boards, legal authorities, or other external entities.

Mandatory Training: Individuals who have violated the AUP might be required to complete specific training related to the misuse as a condition of regaining access or privileges. This can include cybersecurity training, ethics training, or other relevant educational programs.

All Users are expected to cooperate with investigations and audits conducted by the University to ensure Compliance with this policy. The University aims to apply the principles of this policy with fairness and common sense, ensuring due process for all individuals involved.

6. Iterative Improvement and Feedback

Lakehead University is committed to continuously improving this AUP and adapting it to keep pace with technological advancements and emerging security challenges. We recognize that fostering a culture of security, Compliance, and engagement requires active participation from all University Users.

To this end, we encourage ongoing suggestions and feedback from Users regarding the AUP. Feedback can be submitted at any time, not just during formal review periods, to ensure the policy remains relevant and effective in addressing current and future needs.

If you have any suggestions, feedback, or concerns about this policy, please contact the University Secretariat. Your input is invaluable in helping us maintain a secure and compliant IT environment that supports the academic, research, and administrative missions of the University.

Contact for Policy Feedback and Suggestions:

University Secretariat
Location: University Centre, Thunder Bay Campus, Room UC2002
Phone: 807-346-7929
Email: univsec@lakeheadu.ca

By fostering open communication and actively seeking input from our community, we aim to ensure that our IT policies evolve in alignment with best practices and the unique needs of our University.

7. Related Policies, Procedures, Guidelines, Forms

- Electronic Monitoring Policy
- Employee Code of Conduct
- Form for privacy and security review of prospective cloud services contracts
- Information Security Policy
- Intellectual Property Policy
- Research Ethics and Integrity
- Research Data Classification Guidelines
- Residence Community Standards
- Strong Password Standard
- Student Code of Conduct

Review Period: 5 years;
Next Review Period: 2030-2031;
Related Policies and Procedures: See Section 7;
Policies Superseded by this Policy: None.

The University Secretariat manages the development of policies through an impartial, fair governance process, and in accordance with the Policy Governance Framework. Please contact the University Secretariat for additional information on University policies and procedures and/or if you require this information in another format.

Office of the University Secretariat
Hours: Monday through Friday from 8:30am to 4:30pm;
Location: University Centre, Thunder Bay Campus, Room UC2002
Phone: 807-343-8010 ext. 7929
Email: univsec@lakeheadu.ca