Information Technology Acceptable Use Policy

Leech Lake Tribal College - Information Technology

Purpose

The purpose of this Acceptable Use Policy (AUP) is to ensure that the Leech Lake Tribal College (LLTC) Information Technology (IT) environment supports and advances the College's mission of providing high-quality higher education grounded in Anishinaabe values, while protecting the confidentiality, integrity, and availability of institutional systems and data.

This policy establishes expectations for the appropriate, secure, and responsible use of LLTC IT resources to:

- Safeguard institutional, student, and employee information in compliance with applicable legal, regulatory, and tribal requirements
- Promote reliable, secure, and efficient operation of the IT environment
- Ensure IT resources are used in support of academic, administrative, research, and operational objectives
- Enable secure remote work, distance learning, and collaboration
- Define enforcement mechanisms, including investigation of violations and application of appropriate corrective actions

Policy Scope

This policy applies to all aspects of the IT environment for all users, including, but not limited to students, faculty, staff, board of trustees, and third parties. The IT environment includes all IT equipment, systems, networks, devices, and facilities. This policy specifically applies to all LLTC-sponsored websites and social media accounts and is extended to social media content created or posted by members of the LLTC community in a personal capacity if that user created the impression they are posting as part of their role at LLTC

Policy Statement

Use of the IT environment is a privilege, not a right. This Policy is intended to inform IT environment users of their responsibilities and of unacceptable usage. Given the rapid changes in IT, the policy cannot address all potential scenarios. Therefore, users must always keep the purpose of the policy in mind when accessing the IT environment.

The IT environment is administered by the IT Department.

All users are required to comply with this policy and the accompanying rules.

Definitions

Confidential Data: Confidential data includes, but is not limited to, student records, financial information, personally identifiable information (PII), protected research, and proprietary LLTC data. Users must adhere to LLTC data protection guidelines when handling such information to prevent unauthorized disclosure or misuse.

ERP System: An integrated software platform used to manage and automate core institutional business processes by providing a centralized system of record. An ERP system typically supports functions such as finance, human resources, payroll, student or customer records, procurement, and reporting, and enables consistent data management, workflow control, and operational oversight across the organization.

GenAI Tools: Software tools that use generative models leveraging artificial intelligence to generate content. Examples include Microsoft CoPilot, OpenAI, Google Gemini, and Chat GPT.

LLTC IT Environment: The IT environment consists of all *LLTC*-owned and/or operated IT-related equipment, devices, network, servers, storage, IT facilities, software and services. Examples include, but are not limited to, all components of LLTC's computing network, email accounts, cloud-based applications or storage, learning management systems, ERP/student information systems, ancillary applications, and all LLTC-issued PCs, laptops, servers, phones, tablets, etc.

Mass Email Messages: Email messages sent to all students, staff, faculty, or when individual recipient addresses are not defined.

Multifactor Authentication (MFA)*:* An authentication method that requires a user to verify their identity using two or more independent factors from different categories, such as something the user knows (a password or PIN), something the user has (a hardware token, mobile device, or authentication app), or something the user is (biometric characteristics). MFA reduces the risk of unauthorized access by ensuring that compromise of a single authentication factor does not result in access to systems or data.

Users: Individuals currently assigned a computing account by LLTC, or others provided access approved by the LLTC IT Department.

Responsibilities

Password and Authentication

To protect institutional systems and data, all users must comply with the following password and authentication requirements:

- Passwords must be a minimum of twelve (12) characters in length. The use of passphrases is encouraged.

- **Multifactor authentication (MFA)** is required for email, the learning management system (LMS), the Enterprise Resource Planning software (ERP) and all other sensitive institutional systems.
- Password changes are required only when passwords are compromised or when otherwise directed by the IT Department.
- User accounts will be locked after five (5) unsuccessful authentication attempts for a period of fifteen (15) minutes.
- Credentials shall be stored and transmitted using secure, industry-standard cryptographic protections and shall not be stored or transmitted in clear text.
- The use of password managers is permitted and recommended, provided they are approved by or compatible with institutional security standards.
- Password and authentication requirements shall be enforced consistently across institutional systems and monitored by the IT Department.
- Exceptions to password or authentication requirements must be formally approved by the IT Department and the Designated Information Security Officer, documented, and reviewed periodically.
- Password and authentication controls shall be integrated with the account lifecycle, including account creation, modification, inactivity, and termination.
- Privileged accounts shall be subject to stronger authentication controls than non-privileged accounts, commensurate with the elevated risk associated with administrative access.
- Password and authentication requirements shall be reviewed periodically to ensure continued effectiveness and alignment with institutional security and risk considerations.
- Non-privileged accounts will be automatically disabled after 90 days of inactivity.

Privacy, Monitoring, and Ownership

Users have no expectation of privacy when using LLTC computing resources, including but not limited to computer files, email, internet usage, and social media activity conducted through LLTC systems or accounts.

LLTC reserves the right to monitor, access, review, intercept, and disclose electronic communications and system activity at any time, with or without prior notice, to:

- Protect institutional systems and data
- Investigate suspected misconduct or security incidents

- Ensure compliance with institutional policies and legal obligations

Institutional data stored or processed on LLTC systems remains the property of LLTC and must be protected in accordance with institutional security and data classification standards.

Legal, Policy, and Professional Conduct Requirements

Users must:

- Comply with all applicable federal, state, tribal, and local laws
- Adhere to all LLTC policies, including data classification, privacy, confidentiality, and information security requirements
- Conduct themselves professionally and in good taste when using LLTC systems, accounts, and official social media platforms

Acceptable Use of Computing Resources

LLTC computing resources are provided primarily to support academic, administrative, research, and operational activities.

Limited, incidental personal use is permitted only when such use:

- Does not interfere with institutional operations
- Does not consume excessive system or network resources
- Does not violate LLTC policies or applicable laws

Devices, Access, and Security Controls

LLTC-Owned Equipment

Users must:

- Take reasonable steps to prevent damage, loss, or theft of LLTC-owned devices
- Ensure software installations align with IT-approved applications
- Maintain current security patches and updates

Users may be financially responsible for LLTC-owned equipment that is damaged, lost, or stolen due to negligence or failure to comply with institutional requirements, as outlined in applicable equipment agreements.

Personal Devices (BYOD)

Personal devices may be used to access LLTC email only, through approved applications and configurations.

Personal devices may not:

- Store institutional or regulated data locally
- Access internal LLTC systems beyond email
- Connect directly to LLTC networks
- Be used for administrative or non-academic institutional work

Unless explicitly authorized and secured in accordance with LLTC security standards.

Network and Remote Access

- Devices accessing LLTC systems must comply with institutional security policies
- Remote access to LLTC systems must be approved by the user's director and the designated Information Security Officer, and conducted exclusively through the LLTC VPN
- Remote access must only be conducted using an authorized device issued by the LLTC IT Department.
- Unauthorized modification of network protocols (e.g., IP spoofing, network sniffing) is strictly prohibited

LLTC reserves the right to restrict network usage to ensure adequate bandwidth for institutional needs.

Information Protection and Data Handling (GLBA-Aligned)

Users must:

- Protect passwords, credentials, and authentication mechanisms
- Never share accounts or credentials
- Store and transmit confidential or regulated data only using LLTC-approved systems
- Encrypt sensitive data when required
- Follow institutional data retention and disposal policies

Removable Media

- The use of removable media (USB drives, external hard drives, SD cards) on institutional systems is restricted and permitted only for legitimate institutional purposes.
- Unauthorized or personally owned removable media shall not be connected to institutional systems unless explicitly approved.

- Removable media used to store or transfer sensitive or confidential information must be approved, encrypted, and controlled in accordance with institutional security requirements.
- Removable media with unknown ownership or origin is prohibited from use on institutional systems.
- All removable media must be scanned for malicious software prior to use on institutional systems.
- Loss or suspected compromise of removable media must be reported immediately in accordance with the incident response process.

Email and Electronic Communications

Users must:

- Not transmit sensitive or regulated data via email unless encrypted
- Use LLTC-approved collaboration platforms (Microsoft SharePoint and OneDrive) for secure file sharing
- Exercise caution when opening email attachments or links
- Refrain from sending spam, phishing attempts, or malicious content
- Ensure all communications, including limited personal use, maintain professionalism

Mass Email Usage

- Mass email is limited to official institutional communications only.
- Only authorized users or roles may send mass emails, subject to documented approval.
- Mass email shall not be used for personal, commercial, or political purposes.
- Distribution lists must be centrally managed and protected from unauthorized use.
- Mass email content must not include sensitive or confidential information unless explicitly authorized.

Generative Artificial Intelligence (AI) Usage

Permitted Use

Approved generative AI tools may be used for academic, administrative, and operational purposes, provided that:

- AI-generated content is reviewed for accuracy prior to use
- Use complies with all applicable laws and LLTC policies

- AI is not used to automate decision-making without appropriate human oversight

Faculty may establish course-specific requirements governing student use of AI tools.

The use of AI-powered notetaking and meeting transcription tools is prohibited due to privacy, consent, data retention, and information security risks. These tools may capture, store, or transmit sensitive institutional information in ways that are inconsistent with LLTC's data protection, confidentiality, and regulatory obligations.

Prohibited Uses of LLTC Information Technology Resources

The following activities are strictly prohibited when using LLTC information technology resources, systems, networks, accounts, or data, regardless of device ownership or access location.

Unauthorized Access and Credential Misuse

Users must not:

- Attempt to gain access to systems, data, or accounts beyond their authorized permissions, including "browsing" or curiosity-driven access
- Access, use, or attempt to use another person's account
- Share login credentials with any individual or group
- Provide false, misleading, or incomplete information to obtain access to LLTC systems or resources

Interference with Systems and Security Controls

Users must not:

- Disrupt or attempt to disrupt LLTC systems, services, or networks
- Introduce malware, viruses, or malicious code
- Disable, bypass, or circumvent security controls, safeguards, or monitoring mechanisms
- Tunnel unauthorized protocols through firewalls or security devices

Software and System Integrity Violations

Users must not:

- Download, copy, install, or use unauthorized software, applications, or games on LLTC-owned devices
- Modify system configurations or install applications without IT approval

Unauthorized software or applications may be removed by IT without notice.

Misuse of Institutional Data and Information (GLBA / FERPA)

Users must not:

- Access, copy, modify, disclose, or use institutional data without authorization
- Read, delete, copy, forward, or modify another user's email or files without explicit permission
- Post, transmit, or disclose private, restricted, or confidential data except as permitted by policy
- Use private or restricted data, as defined in the LLTC Data Classification Policy, with generative AI tools without written approval from the Data Governance Committee and Designated Information Security Officer.

Prohibited Communications and Content

Users must not use LLTC systems or accounts to:

- Harass, intimidate, threaten, defame, or discriminate against any individual or group
- Transmit obscene, profane, lewd, vulgar, inflammatory, or disrespectful content
- Post or transmit false, misleading, or defamatory information about individuals or organizations
- Disclose private or personal information about another individual without authorization

Violations involving harassment or discrimination based on protected classifications are subject to LLTC's harassment and nondiscrimination policies.

Email Abuse and Messaging Misconduct

Users must not:

- Send unsolicited, unwanted, or bulk email messages unrelated to legitimate academic or administrative activities
- Send spam, junk mail, chain letters, mail bombs, or advertising messages without authorization
- Use false identities, aliases, or spoofed addresses when sending messages
- Transmit threatening or malicious communications

Network Resource Abuse

Users must not:

- Use LLTC systems or networks in a manner that degrades performance, availability, or accessibility
- Consume excessive bandwidth for non-institutional purposes
- Engage in activities that interfere with the normal operation of institutional services

Commercial, Political, and Personal Gain Activities

Users must not:

- Use LLTC systems, email, or websites to solicit for commercial ventures, personal business activities, or personal financial gain
- Use LLTC resources to promote religious or political causes, candidates, or organizations
- Offer goods or services of a commercial nature using LLTC systems, except where consistent with LLTC's mission and explicitly authorized

Social Media Misrepresentation and Misuse

Users must not:

- Use the LLTC name, logo, or image to endorse opinions, products, causes, businesses, or political candidates without authorization
- Use social media in a manner that falsely implies representation of LLTC
- Disclose confidential, proprietary, or regulated institutional information via social media

Compliance and Enforcement

Users who violate this policy may be denied access to institution computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the institution with disciplinary procedures applicable to the user. The institution may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of institution or other computing resources or to protect the institution from liability. The institution may also refer suspected violations of applicable law to appropriate law enforcement agencies.

References and Resources

LLTC Data Governance Policy
LLTC Data Classification Policy
LTTC Cybersecurity and Privacy Training Policy
LLTC Privacy Statement and Policy

Policy Revision and Approval History

Name	Date	Description of Change	Version Number
Jeremy Bennett	12/27/2025	Document Creation	1.0
Data Governance Committee	01/12/2026 01/26/2026	Document Review and Update	1.0
Sent to the Policy Review Committee	02/05/2026	Final Review and Committee Approval	1.0
Policy Approved by the HR Policy Committee	2/10/2026	Policy Review and Implementation: Ready to be sent to BOT Policy Sub-Committee	1.0
Policy Sent to BOT Policy Subcommittee	2/10/2026	Policy Review and Ready for BOT Review	1.0
Policy Subcommittee Review	2/19/2026	Recommend moving to BOT for final review	1.0
BOT Policy Review	2/23/2026	Final Policy Review	1.0
Revisions Needed	NA`	None needed	1.0
Policy Approval and Implementation Date	2/23/2026	Final Approval and Implementation Date	1.0