

LLTC Data Privacy Statement and Policy

Leech Lake Tribal College – IT, DAIR, Registrar

Purpose

Leech Lake Tribal College (LLTC) is committed to protecting the privacy and security of personal data collected from students, faculty, staff, and our Leech Lake Band of Ojibwe (LLBO) community members. This statement applies to all individuals whose personal information is collected, accessed, stored, or processed by LLTC, including through our website, systems, and institutional activities.

Policy Scope:

A. Institutional Coverage

This policy applies to all departments, programs, offices, and operational units of Leech Lake Tribal College, including but not limited to: Academics, Student Services, Advising, Finance, and Financial Aid. Information Technology, Human Resources, Institutional Research and Assessment, Library and Learning Resources, and any LLTC-affiliated centers, grants, contracts, and sponsored programs.

B. Individuals Covered

This policy applies to all individuals who create, access, store, process, manage, transmit, or dispose of LLTC data, including full-time and part-time employees, faculty and adjunct instructors, student workers, contractors, vendors, and consultants, volunteers, board members and any external partners or entities granted access to LLTC systems or data.

C. Data Covered

This policy covers all data created, collected, stored, processed, or transmitted by LLTC, regardless of format or system, including but not limited to:

1. Personally Identifiable Information (PII), student records and educational data (FERPA-protected), employee personnel information, financial, payroll, and benefits information, contact details, demographic information, or any data that identifies an individual.

2. Sensitive Institutional Data

Financial and accounting records, research, assessment, and accreditation data, grant-funded project data, internal reports, planning documents, and proprietary materials.

3. Technology and System Data

Data stored in LLTC servers, databases, cloud systems, applications, websites, and learning platforms, network activity logs, authentication data, and system access records.

4. Physical and Digital Formats

This policy applies to data regardless of: Format (digital, paper, audio, video), storage location (on-premise, cloud-based, mobile device, external drive), method of transmission (email, file-sharing, physical transport, etc.).

D. Activities Covered

This policy applies to all data-related activities, including: Collection and creation, access and use, storage and retention, transmission, sharing or disclosure, archiving and backup, disposal or destruction.

3. Exclusions

This policy does not apply to: Personal data stored by individuals for non-LLTC purposes, publicly available institutional information already designated for open dissemination, data protected under specific external regulations (HIPAA data from external healthcare providers) unless the data resides within LLTC systems.

4. Relationship to Other Policies

This scope aligns with and complements: LLTC Information Technology Acceptable Use Policy, FERPA compliance policies, records retention schedules, grant-funded data security requirements, and institutional research ethics and data governance policies.

2. Definitions

- **Personal Data:** Any information relating to an identifiable person, including but not limited to name, contact details, academic records, and financial information.
- **Tribal Data:** Information that pertains to the LLTC community, grounded in Indigenous values and governed by the principle of Indigenous data sovereignty as inherent to tribal nations.
- **Research:** Research at Leech Lake Tribal College refers to any systematic process of inquiry conducted for the purpose of improving institutional practices, understanding student learning, strengthening programs, or supporting community-driven knowledge development. At LLTC, research does *not* involve human subjects research requiring federal IRB oversight or CITI training, but instead includes activities such as:
 - A. Collecting and analyzing institutional data (enrollment, retention, assessment results) to improve programs and services.
 - B. Evaluations, surveys, or studies conducted for internal planning, accreditation, or accountability purposes.

- C. Curriculum-related inquiry, such as faculty-led classroom assessments or explorations of teaching and learning practices.
- D. Community-engaged inquiry aligned with Anishinaabe values, cultural knowledge, or Tribal priorities, conducted in collaboration with Tribal departments or community partners.
- E. Grant-required reporting or assessment projects that examine program performance or student outcomes.

Research at LLTC does not include activities that meet the federal definition of human subjects' research requiring IRB approval, unless conducted through an external partner with appropriate oversight.

3. Principles of Indigenous Data Sovereignty

- LLTC recognizes its authority to govern the collection, ownership, and use of its data in alignment with tribal values and sovereignty.
- All data activities will advance the well-being of the LLTC community and respect cultural data sensitivities.
- Consent requirements will be clear, informed, culturally respectful, and can be withdrawn at any time.

4. Legal & Regulatory Compliance

LLTC adheres to applicable federal and state laws, including:

- **FERPA:** Ensures the confidentiality of student educational records and grants rights to access and control their disclosure.
- **HIPAA:** Applies where LLTC processes protected health information (PHI).
- **Title IX:** Applies where LLTC processes reports of
- State privacy laws, to the extent they apply to public or private tribal institutions.

5. Data Collection & Usage

LLTC collects personal data:

- To support admissions, academic advising, student services, and research.
- To fulfill accreditation requirements for agency and regulatory reporting.
- To deliver institutional communications and alerts.

Data uses will be limited to clearly stated purposes, minimized, and retained as required.

6. Data Sharing & Third Parties

- LLTC may share data with partners or service providers (e.g., student information systems, or learning management platforms), only under strict privacy agreements ensuring compliance.
- Tribal and student data will not be shared without informed consent, unless legally required.

7. Rights & Controls

- Students and employees have rights to access, correct, and request deletion of their personal data, as permitted under law. Refer to: FERPA Federal website.
- Institutional partners or leadership can withdraw consent for certain data uses.
- Requests to change student information can be made to the Registrar/FERPA Officer.

8. Data Security

LLTC follows industry standards (e.g., NIST, CIS) and internal protocols for secure data storage, access controls, incident response, and employee training.

9. Information Technology (IT) & Digital Security

LLTC's IT Department plays a critical role in safeguarding institutional and personal data.

- **System Security:** All LLTC systems use encryption, firewalls, and multi-factor authentication to protect data.
- **Network Monitoring:** Continuous monitoring detects and mitigates unauthorized access or suspicious activity.
- **Access Management:** Role-based access ensures that only authorized personnel can view or modify sensitive data.
- **Device Security:** College-owned devices must comply with security protocols, including regular updates and antivirus protection.
- **Incident Response:** The IT Incident Response Team will promptly investigate and remediate any data breach or cyber threat, notifying affected individuals as required by law.
- **Training & Awareness:** LLTC provides regular cybersecurity training for staff, faculty, and students to promote safe digital practices. (Reference: Cybersecurity and Privacy Training Policy).

10. Policy Updates

This statement may be revised periodically to reflect legal changes, technological developments, or tribal community priorities.

11. Accountability & Governance

The Data Governance Committee oversees the overall compliance, policy reviews, and community engagement to ensure alignment with college and tribal initiatives.

- The Information Security Officer or equivalent will oversee direct policy implementation and compliance.
- Regular policy reviews, audits, and community engagement will ensure alignment with institutional and tribal initiatives.
- Mentorship of data practices will reflect transparency, cultural respect, and community partnership.

10. Policy Updates

This statement may be revised periodically to reflect legal changes, technological developments, or tribal community initiatives. LLTC will provide timely notice of updates.

11. Contact Information

For privacy inquiries, consent requests, or data concerns, please contact:

Role: Information Security Officer

Email: privacy@lltc.edu

Phone: (218) 335-4200

References and Resources

LLTC Data Governance Policy

LLTC Data Classification Policy

LTTC Cybersecurity and Privacy Training Policy

Revision History

Name	Date	Description of Change	Version Number
Dr. Tracy Diefenbach	12/27/2026	Document Creation	1.0
Data Governance Committee	01/27/2026	Final Draft Approval	1.0
Sent to the Policy Review Committee	02/05/2026	Seeking Final Policy Approval and Implementation	1.0
Policy Approved	TBD	Final Policy Approval and Implementation.	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	TBD	1.0
BOT Policy Review	2/23/206	Final Policy Review	1.0
Revisions Needed	NA	None needed or recommended	1.0
Policy Approval and Implementation Date	2/23/2026	Final Approval and Implementation Date	1.0