

Institutional Data Governance Policy

Leech Lake Tribal College: Assessment and Research

Purpose

LLTC's mission is grounded in Anishinaabe values; this policy ensures that LLTC data are governed ethically, lawfully, and in accordance with tribal sovereignty, Indigenous data governance principles, and U.S. higher education regulations. It integrates:

- **CARE Principles** (Collective Benefit, Authority to Control, Responsibility, Ethics), prioritizing people and purpose alongside FAIR data movements.
- **OCAP Principles** (Ownership, Control, Access, Possession), asserting Anishinaabe/Ojibwe's collective rights in the collection, use, and stewardship of Indigenous data.
- **FERPA** protections for student education records (including treatment records at postsecondary institutions).
- **HIPAA/FERPA Joint Guidance** for student health records and when HIPAA may or may not apply in campus contexts.
- **GLBA Safeguards Rule** for Title IV institutions (security of nonpublic personal information).
- **NIST Privacy Framework** (Identify-P, Govern-P, Control-P, Communicate-P, Protect-P) for risk-based privacy management. Comply with regulatory requirements and best practices.
- Higher-education data governance and classification practices (EDUCAUSE).

Policy Scope: This policy applies to all LLTC staff, faculty, students, third party data-collectors or servicers, or anyone collecting, using, publishing, or reporting on LLTC institutional data.

Policy Statement: This policy complements LLTC's Charter and the Director of Assessment & Institutional Research's role as the central repository for institutional data. This policy also serves as part I of the Institutional Assessment Handbook and Data Governance Plan.

Definitions

- **Institutional Data:** Any information created, received, maintained, or transmitted in the conduct of LLTC operations (e.g., student records, HR/payroll, finance, accreditation). FERPA defines "education records" broadly as records directly related to a student and maintained by the institution.
- **Cultural/Indigenous Data:** Knowledge and information about Indigenous Peoples, including languages, practices, protocols, stories, ceremonies, genealogies, place-based

knowledge, and traditional ecological knowledge considered collectively owned and governed under tribal sovereignty.

- **Sensitive Financial Information:** Nonpublic personal information (NPI) subject to GLBA Safeguards Rule (e.g., SSNs, bank details, financial aid records).
- **Data Owner:** Role responsible for the quality, classification, access decisions, and lifecycle of data domains. (EDUCAUSE practice) (Separate SOP or policy)
- **Data Custodian:** IT/ISO role responsible for technical safeguards and systems containing data. (EDUCAUSE practice)

Governance Structure

3.1 Data Governance Committee (DGC)

A cross-functional body chartered by the LLTC staff to set policy, resolve escalations, and ensure compliance with tribal sovereignty and federal regulations. Members:

- Chair: Director of Assessment & Institutional Research (DAIR).
- Registrar (FERPA subject matter lead).
- CIO/IT/ (GLBA/NIST implementation and compliance lead).
- Financial Aid Director (GLBA Safeguards compliance).
- Faculty Council (research/academic data). (EDUCAUSE) governance patterns).
- Cultural Committee representatives, appointed by LLTC leadership in consultation with Leech Lake Band of Ojibwe (LLBO). (CARE/OCAP operationalization) (Extension).
- Legal Counsel (policy alignment with LLBO codes and U.S. regulations).

3.2 Cultural Committee

Reports to DGC. Reviews any proposal involving Indigenous data for CARE/OCAP alignment, cultural risk, and benefit-sharing; may impose conditions or deny requests.

3.3 Data Owners & Custodians

Each major domain (Student, HR, Finance, Research, Advancement, Library, Cultural Archives, Financial Aid) has a named (owner) and custodian (technical owner).

Indigenous Data Sovereignty Commitments

LLTC recognizes LLBO's inherent sovereignty and the collective rights attached to Indigenous data. LLTC commits to:

1. **Collective Benefit:** Ensure data use yields equitable, community-defined benefits; avoid extractive practices.

2. **Authority to Control:** Honor tribal authority over Indigenous data, including review and veto power via the cultural committee and the data governance committee.
3. **Responsibility:** Build relationships; minimize harm; provide transparency and accountability in data use.
4. **Ethics:** Apply cultural protocols; protect sensitive knowledge; consider future impacts.
5. **OCAP Operationalization:** Treat Indigenous data as collectively owned; ensure tribal control over research lifecycle; provide tribal access; honor and maintain holistic balance where appropriate.

LLTC will align with LLBO's Data Sovereignty outcomes and tribal codes as they are published.

Legal & Regulatory Alignment

- **FERPA:** LLTC will protect student education records, require consent for disclosure except under defined exceptions (e.g., school officials with legitimate educational interest; emergencies), and maintain annual notices.
- **HIPAA/FERPA:** Student health/clinic records at postsecondary institutions are generally FERPA education or treatment records, excluded from HIPAA PHI; HIPAA may apply when services are provided by external covered entities (e.g., hospital partner).
- **GLBA Safeguards Rule:** As a Title IV institution, LLTC must implement an information security program for NPI; designate qualified individual; conduct risk assessments; implement safeguards; train staff; monitor and test; incident response; Board reporting.
- **NIST Privacy Framework:** LLTC will use the NIST PF functions to manage privacy risk across data processing: Identify-P, Govern-P, Control-P, Communicate-P, Protect-P.

6) Data Classification

LLTC adopts two complementary schemas: Institutional Classification (risk/security) and Cultural Sensitivity Classification (sovereignty/ethics)

6.1 Institutional Risk Levels (examples)

- **Public:** Approved for public release (example: website content, published reports).
- **Internal:** Routine internal documents not for public distribution.
- **Sensitive:** Student records (FERPA), HR files, internal financials.
- **Restricted:** NPI (GLBA), SSNs, health treatment records, credentials, security keys.

6.2 Cultural Sensitivity Levels (examples)

- **C1: General Cultural Content:** Already public, educational.

- **C2: Community-Shared Knowledge:** Requires respectful context; local partnerships. (CARE/Responsibility)
- **C3: Restricted Traditional Knowledge:** Protocol-bound; requires the cultural committee and DGC approval; stringent access controls; may require tribal custodian safekeeping. (OCAP safekeeping)
- **C4: Sacred/Highly Sensitive Knowledge:** Access extremely limited; may never be digitized or stored on general systems; governed solely by cultural protocols and tribal authority. (CARE Ethics; OCAP Ownership/Control)

6.3 Roles & Responsibilities

- **DGC (Data Governance Committee):** Approves policies/standards; arbitrates conflicts; receives compliance reports (GLBA/NIST/FERPA).
- **Cultural Committee:** Reviews cultural data activities; ensures CARE/OCAP compliance; sets benefit-sharing terms; approves cultural data sharing agreements.
- **Data Owners:** Classify data; define access roles; ensure quality and lifecycle actions; coordinate with Custodians.
- **Data Custodians (IT):** Implement technical controls (encryption, MFA, backups, monitoring); maintain systems per GLBA/NIST.
- **Researchers/Faculty/Staff:** Comply with policy; obtain approvals; follow cultural protocols; protect student and cultural data. (EDUCAUSE culture of data)
- **DAIR (Director of Assessment and Institutional Research):** Acts as central repository; coordinates institutional reporting and data catalog; leads training and audits. (TEAMS)

8) Access & Use

- **Role-Based Access Control (RBAC):** Access granted by Owner; least privilege; logging and periodic recertification. (GLBA/NIST practice)
- **FERPA Access and Title IX (Vector Solutions)** Limited to school officials with legitimate educational interest; directory information only per published notice.
- **Cultural Data Access:** Determined by Cultural Committee in accordance with tribal protocols; may require community consultation, embargoes, or physical custody by a tribal archive. (CARE/OCAP)

Data Lifecycle Management

9.1 Collection:

- Collect minimum necessary; obtain informed consent when appropriate; disclose intended uses and benefit-sharing for Indigenous data. (CARE Responsibility/Ethics)

- For AI, please refer to LLTC's General Acceptable Use policy).

9.2 Storage & Security:

- Encrypt Sensitive/Restricted data at rest and in transit; require MFA; segment networks; maintain backups; monitor for anomalies; patch systems. (GLBA Safeguards; EDUCAUSE security practices).
- Storage timelines will be based on department requirements.

9.3 Quality & Metadata:

- Maintain provenance, lineage, and definitions; tag datasets with both institutional risk and cultural sensitivity levels; publish in a governed data catalog. (EDUCAUSE modernization).

9.4 Sharing & Publication:

- Require **Data Sharing Agreements** (DSAs) for any external sharing; DGC and Cultural Committee approval for cultural datasets; incorporate CARE/OCAP clauses (collective benefit, control, access, possession), disclosure limits, benefit-sharing, and takedown rights. (CARE, OCAP, Tribal data sharing templates)

9.5 Retention & Disposal:

- Retain per legal/academic requirements; for Indigenous data, retention is set by tribal protocols and the DGC; dispose securely (sanitization, certificate of destruction). (GLBA disposal; EDUCAUSE checklists). (5-year minimum lifecycle requirement of all institutional data unless otherwise specified by a local, state, or federal regulatory body)

10) Research Involving Indigenous Data

- **Research Review:** All projects using Indigenous data must obtain DGC approval and, where applicable, LLBO review per Education Code as appropriate.
- **Agreements:** Require DSAs and Memoranda of Understanding specifying OCAP/CARE, IP rights, community review, and publication controls.
- **Outputs:** Community co-authorship encouraged; embargoes or non-publication may be conditions; derivative AI training on cultural data is prohibited without explicit tribal authorization. (CARE Ethics/Authority to Control).

11) Training & Awareness

- Annual training for all employees on FERPA, GLBA Safeguards, privacy, cybersecurity hygiene, and Indigenous data governance (CARE/OCAP). (EDUCAUSE awareness; GLBA training requirement) (Referral Policy: Cybersecurity Awareness and Privacy Training Policy).

- Specialized workshops for faculty/researchers on cultural protocols, DSAs, and community engagement. (CARE Responsibility) This shall include student training on proper use of institutional data for on and off-campus research projects, publishing, and reporting.

12) Incident Response & Breach Notification

LLTC maintains a written **Incident Response Plan** with incident response procedures covering:

- Identification, containment, eradication, recovery, and post-incident review.
- Notification obligations under FERPA (as applicable), GLBA, and tribal agreements.
- Immediate notification to DGC, and the Cultural Committee (for cultural data), and LLBO authorities as mandated by DSAs. (GLBA Safeguards; NIST PF Protect-P/Communicate-P).

Data Sharing Agreements (DSA) Minimum Clauses

All DSAs, especially those involving Indigenous data must include:

1. **Purpose & Collective Benefit** (CARE).
2. **Authority to Control & Governance**: tribal review and veto; DGC oversight.
3. **Ownership & Possession/Stewardship** (OCAP).
4. **Access Controls, Use Limitations, Redisclosure Prohibition** (FERPA/GLBA).
5. **Security Controls** (encryption, MFA, monitoring).
6. **Benefit-Sharing & Acknowledgment** (CARE).
7. **Retention & Disposal** (per tribal protocols and law).
8. **Breach Notification & Remedies** (GLBA/NIST).

14) AI, Analytics, and Secondary Use

- Any AI training or analytics using Indigenous or student data requires DGC approval and committee review; de-identification is not sufficient if cultural meaning or re-identification risk persists. (CARE Ethics; NIST Identify-P/Govern-P)
- Prohibit use of sacred/Highly Sensitive (C4) datasets for model training unless explicitly authorized by tribal authority under a DSA. (OCAP Control/Possession)

15) Transparency & Individual Rights

- Publish privacy notices; maintain a catalog of public datasets; honor FERPA rights to inspect, amend, and consent (or eligible student rights at age 18/postsecondary).

- For Indigenous data, LLTC commits to culturally appropriate communication and community consultation before public dissemination. (CARE Communicate/Ethics)

16) Compliance, Audit & Continuous Improvement

- Annual compliance review (FERPA, GLBA Safeguards, NIST PF), with reports to DGC and LLTC Board.
- Maturity assessments against EDUCAUSE governance practices and NIST PF Implementation Tiers.

17) Enforcement

Violations may result in disciplinary action, termination of research privileges, and reporting to designated authorities. LLTC reserves the right to suspend access to any systems pending investigation, and to enforce tribal directives regarding Indigenous data. (GLBA enforcement implications; FERPA funding risk)

18) Related Documents & References (References for Data Governance Policies).

- LLTC Charter; DAIR Vision/Role.
- LLBO Data Sovereignty Project (2023-present).
- CARE Principles—Global Indigenous Data Alliance
- OCAP®—First Nations Information Governance Centre.
- FERPA regulations and guidance (US ED; CDC).
- HIPAA/FERPA joint guidance (US ED/HHS).
- GLBA Safeguards for higher education (FTC; DOE presentations; law firm and association guides) and the NIST Privacy Framework.
- EDUCAUSE resources on data governance and classification.

References and Resources

LLTC Data Governance Policy

LLTC Data Classification Policy

LTTC Cybersecurity and Privacy Training Policy

LLTC Privacy Policy

Revision History

Name	Date	Description of Change	Version Number
Dr. Tracy Diefenbach	10/06/2025	Document Creation	1.0
Data Governance Committee	01/27/2026	Final Draft Approval	1.0
Sent to Policy Review Committee	02/05/2026	Seeking final approval and implementation for this policy	1.0
Final Policy Approval	TBD	Final approval and policy implementation	1.0