

**Leech Lake Tribal College (LLTC):  
Data Collection Policy: Internal and External Requests**

**Owner:** Director of Assessment & Institutional Research (DAIR)

**Co-Owners:** Information Technology (IT), Registrar, Institutional Review Board (IRB)

**Review Cycle:** Annual (each July)

**Purpose**

Leech Lake Tribal College (LLTC) is committed to protecting the privacy, security, and sovereignty of data about our students, employees, partners, culture, and communities. This policy establishes consistent procedures for requesting, approving, collecting, sharing, and reporting LLTC data for internal and external purposes, including Memoranda of Agreement (MOAs), Data Sharing Agreements (DSAs), and third-party requests. It ensures compliance with applicable laws (e.g., FERP, HIPAA, PII, PHI, GLBA), accreditation and grant obligations, LLTC's cultural protocols, and Indigenous Data Sovereignty and Infrastructure principles.

**Scope**

This policy applies to all LLTC data, student, employee, academic, operational, financial, facilities, cultural, and research data, regardless of format or system (SIS, LMS, HRIS, CRM, data warehouse, spreadsheets, etc.). It covers:

- Internal data requests by LLTC personnel and units.
- External data requests by third parties (e.g., researchers, vendors, funders, agencies, other institutions).
- MOAs/DSAs governing ongoing or one-time data exchanges.
- Research-related data collection and use requiring IRB oversight.
- Surveys administered to LLTC and LLBO community populations.
- Public reporting and de-identified data releases, or publications using LLTC's data.

**Policy Principles**

1. **Legal Compliance & Ethics:** Adhere to FERPA and other applicable federal, state, tribal, and grant/contract requirements.
2. **Indigenous Data Sovereignty:** Data about LLTC and the LLBO community is a cultural asset. Stewardship centers community benefit, collective consent, accountability, and reciprocity.
3. **Data Minimization:** Collect and share only what is necessary for a legitimate purpose.
4. **Protection & Security:** Classify data and apply access controls, secure transfer, and appropriate retention/disposal.

5. **Transparency & Accountability:** Decisions are documented and auditable; data subjects' rights and LLTC's obligations are respected.
6. **Data Quality:** Ensure accuracy, integrity, timeliness, and proper interpretation.

### Roles & Responsibilities

- **Board of Trustees:** Adopts institution-wide data governance principles and delegates authority for policy implementation.
- **President/Administration:** Ensures resources, oversight, and cross-unit adherence.
- **Data Governance Committee (DGC):** Interprets this policy, resolves escalations, approves high-risk requests, and maintains data classification and standards.
- **Director of Assessment & Institutional Research (DAIR):** Policy owner; coordinates intake, review, approvals, fulfillment, and metric reporting.
- **Registrar:** Custodian of education records; co-approves student-level releases; ensures FERPA compliance.
- **IRB:** Reviews research activities involving human participants or sensitive LLTC data; may require protocol approval prior to data release.
- **IT/Security:** Ensures technical safeguards, secure transfer, breach response, and vendor risk assessment.
- **Data Stewards (Functional Owners):** Validate definitions, quality, and appropriateness for release (e.g., Finance for financial data).
- **Requestors (Internal/External):** Provide complete justifications, limit use, protect data, and comply with terms.

### Data Classification

- **Restricted (Highly Sensitive):** Direct identifiers (SSN, full DOB, SSN-linked IDs), health data, disability status, tribal enrollment information, financial account data, authentication credentials.
- **Confidential (Sensitive):** Student education records (non-directory), course-level outcomes, advising notes, HR personnel data, detailed financials.
- **Internal:** Aggregate, de-identified, or non-public operational data used within LLTC.
- **Public:** Approved, published statistics (e.g., factbook indicators), policy documents, publicly posted reports.

### Request Channels & When to Use Them

- **Internal Requests:** Use the LLTC Data Request Form for operational analysis, accreditation, grant reporting, program review, assessment, and dashboards.

- **External/Third-Party Requests:** Use the External Data Request Form; if recurring or involving PII/PHI/sensitive data, an MOA/DSA and IRB (if research) are required.
- **Research Involving Human Participants or Surveys:** Submit **IRB Protocol** first; DAIR will not release data until IRB clearance (or exemption) is documented with CITI certification/training on record with LLTC.
- **Vendor Integrations/Tools:** Trigger Vendor Risk/Security Review and DSA prior to any data exchange.

### Standard Decision Criteria

Requests are evaluated against:

1. **Purpose Fit:** Clear legitimate educational interest, research merit, or institutional need.
2. **Minimum Necessary:** Data elements scoped to the least amount needed.
3. **Risk Level:** Sensitivity, identifiability, re-identification risk, data linkage risk, and recipient safeguards.
4. **Compliance:** FERPA, IRB determination, grant/contract terms, tribal/LLTC policies.
5. **Sovereignty & Benefit:** Benefit to LLTC and community, alignment with cultural protocols, reciprocity (results sharing).
6. **Feasibility & Effort:** Time, cost, capacity, data quality constraints.

### Approval Matrix

- **Low-Risk Aggregates (External or Internal):** DAIR and the Data Stewards.
- **Student-Level Confidential Data:**( DAIR, Registrar, Data Steward; notify DGC for unusual scopes).
- **Restricted/Highly Sensitive or Cross-System Extracts:** (DAIR, Registrar (if student records) then IT/Security to the Data Steward and DGC approval)
- **Indigenous Data** (Data Governance Committee, Cultural Committee, DAIR, and the Data Steward).
- **External Third Parties (any PII/sensitive):** (DAIR, Registrar, IT/Security, and Legal/Administration then the DGC); MOA/DSA required.
- **Research with Human Participants:** **IRB approval/exemption required** prior to release; then follow the appropriate tier above.

### Required Agreements

#### Memorandum of Agreement (MOA) / Data Sharing Agreement (DSA)

For ongoing or substantive exchanges, the MOA/DSA must specify:

- Parties, purpose, legal authority, and term.
- Exact data elements and data classification.
- Use limitations; prohibition on redisclosure.
- Security controls (encryption at rest/in transit, access, storage location).
- De-identification/pseudonymization requirements where applicable.
- Retention period and destruction/certification timeline.
- Incident/breach notification timelines and procedures.
- Audit and right to request usage logs.
- Attribution, publication, and review requirements (LLTC review prior to release).
- Compliance with FERPA and LLTC Indigenous Data Sovereignty principles.
- Points of contact and change management.

### **IRB & Research Terms**

Where research is involved:

- IRB protocol approval or special-committee exemption is required before data release.
- Consent language must align with intended data use; secondary use requires additional review.
- Publications must avoid reidentification and respect cultural protocols; LLTC may require pre-publication review in MOA/DSA.

### **Data Preparation & Privacy Techniques**

- **De-identification:** Remove direct identifiers; apply k-anonymity thresholds (suppress cell sizes less than 10), top/bottom coding, category banding.
- **Aggregation:** Report summaries (means, medians, rates) rather than row-level data whenever feasible.
- **Data Dictionaries & Footnotes:** Include definitions, cohorts, terms, time frames, and caveats.
- **Quality Checks:** Validate joins, date ranges, outliers, and denominator logic before release.

### **Secure Transfer & Storage**

- Approved methods: SFTP (SSH File Transfer Protocol), encrypted SharePoint/OneDrive with restricted permissions, or approved vendor secure portals.
- Prohibited methods: Unencrypted email attachments or personal cloud storage.
- External recipients must implement access controls, endpoint protections, and encryption; attestations may be required.

### **Retention & Destruction**

- Retain only for the period defined in the request or MOA/DSA. (Minimum of three years for all institutional data).
- External parties must certify destruction upon term completion or project end.
- LLTC follows its records retention schedule; DAIR coordinates archival and purge procedures with IT and the Registrar.

### **Publication & Attribution**

- Public releases (dashboards, factbooks, briefs) require DAIR review for accuracy and disclosure risk.

- External publications using LLTC data require acknowledgment language approved by DAIR/Administration and may require pre-publication review per MOA/DSA.

#### **Surveys & Contact with LLTC Populations**

- External surveys require IRB review and DAIR scheduling to minimize survey fatigue.
- Email/text outreach to LLTC lists must be coordinated with DAIR and Communications; opt-out and privacy notices required.

#### **Breach, Incident, & Non-Compliance**

- **Report immediately** to DAIR and IT/Security if data is lost, misdirected, or accessed improperly.
- DAIR, IT, and Administration will initiate incident response, notification, and mitigation steps per LLTC Incident Response procedures.
- Non-compliance may result in revocation of access, disciplinary action, and termination of agreements.

#### **Appeals & Escalation**

- Requestors may appeal denials to the DGC in writing within ten (10) business days.
- The DGC decision is final unless legal or accreditation obligations require modification.

#### **Training & Awareness**

- Annual training is required for data stewards and frequent requestors (FERPA, security, Indigenous Data Sovereignty, suppression standards).
- New MOAs/DSAs trigger brief onboarding for recipients on permitted uses and safeguards.

#### **Metrics & Continuous Improvement**

- DAIR maintains a registry of requests (type, turnaround, risk category, disposition).
- Quarterly summaries go to the DGC; the policy and forms are updated annually.

#### **Revision History**

| <b>Name</b>                            | <b>Date</b> | <b>Description of Change</b>                                 | <b>Version Number</b> |
|----------------------------------------|-------------|--------------------------------------------------------------|-----------------------|
| Dr. Tracy Diefenbach                   | 03/01/2026  | Document Creation                                            | 1.0                   |
| Data Governance Committee              | 04/13/2026  | Draft Approval: Voted to move forward to HR Policy Committee | 1.0                   |
| Sent to the HR Policy Review Committee | 4/20/2026   | Seeking Final Policy Approval and Implementation             | 1.0                   |

Data Collection Policy: Internal and External Requests\_Draft\_2026 6

|                                                                                    |                        |                                                                                                   |     |
|------------------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------|-----|
| Retracted from HR Policy Committee to make corrections to Definitions and Headings | 4/24/2026<br>6/26/2026 | Sent a Teams message to HR to retract the draft version, and sent the actual version on 4/24/2026 | 1.0 |
| HR Policy Committee                                                                | 7/21/2026              | Approved to move forward                                                                          | 1.0 |
| Policy Approved                                                                    | 7/23/2026              | Final Policy Approval and Implementation.                                                         | 1.0 |
|                                                                                    |                        |                                                                                                   |     |

**Appendix A: Internal Data Request Form (Summary of Fields)**

| LLTC INTERNAL DATA REQUEST FORM                                                      |                                                           |                 |            |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------|-----------------|------------|
| Policy Reference                                                                     | LLTC Data Collection Policy: Internal & External Requests | Submission Date | 2026-03-16 |
| <b>SECTION 1: REQUESTOR DETAILS</b>                                                  |                                                           |                 |            |
| Requestor Name*                                                                      |                                                           |                 |            |
| Department/Unit*                                                                     |                                                           |                 |            |
| Supervisor Name*                                                                     |                                                           |                 |            |
| Supervisor Approval*                                                                 |                                                           |                 |            |
| Email*                                                                               |                                                           |                 |            |
| Phone                                                                                |                                                           |                 |            |
| <b>SECTION 2: PURPOSE &amp; INTENDED USE</b>                                         |                                                           |                 |            |
| Purpose & Decision to be Informed*                                                   |                                                           |                 |            |
| Intended Use (e.g., assessment, accreditation, grant, program review)*               |                                                           |                 |            |
| Deadline (YYYY-MM-DD)*                                                               |                                                           |                 |            |
| Funding/Contract Reference (if any)                                                  |                                                           |                 |            |
| <b>SECTION 3: POPULATION, TIMEFRAME, &amp; SYSTEMS</b>                               |                                                           |                 |            |
| Data Subjects* (e.g., all students, first-time freshmen, employees)                  |                                                           |                 |            |
| Timeframe/Cohort* (e.g., FA2024, AY2024-25)                                          |                                                           |                 |            |
| Systems to Query (e.g., SIS, LMS, HRIS)                                              |                                                           |                 |            |
| <b>SECTION 4: SPECIFIC DATA ELEMENTS REQUESTED</b>                                   |                                                           |                 |            |
| List each field needed (minimize to essentials). Attach a spec if helpful.           |                                                           |                 |            |
| <b>SECTION 5: SENSITIVITY LEVEL &amp; PROTECTIONS</b>                                |                                                           |                 |            |
| Sensitivity Level*                                                                   |                                                           |                 |            |
| Proposed Protections (storage, access controls, encryption)*                         |                                                           |                 |            |
| <b>SECTION 6: DISTRIBUTION &amp; STORAGE</b>                                         |                                                           |                 |            |
| Who will receive the data? (names/emails)*                                           |                                                           |                 |            |
| Storage Location* (e.g., LLTC SharePoint path, OneDrive with restricted permissions) |                                                           |                 |            |
| <b>SECTION 7: PUBLICATION &amp; IRB STATUS</b>                                       |                                                           |                 |            |

## Data Collection Policy: Internal and External Requests\_Draft\_2026 8

Will results be published or publicly shared?\*

IRB Status (if research or surveys)

IRB Protocol # (if applicable)

|  |
|--|
|  |
|  |
|  |

### SECTION 8: CERTIFICATIONS

I certify this request follows the Minimum Necessary principle and I agree not to redisclose data.

Requested Destruction/Retention Date (YYYY-MM-DD)\*

Requestor Signature (type full name)\*

|  |
|--|
|  |
|  |

Appendix B: External Data Request Form (Summary of Fields)

| LLTC EXTERNAL DATA REQUEST FORM |                                                           |                 |            |
|---------------------------------|-----------------------------------------------------------|-----------------|------------|
| Policy Reference                | LLTC Data Collection Policy: Internal & External Requests | Submission Date | 2026-03-16 |

SECTION 1: ORGANIZATION & CONTACT DETAILS

|                                                                |  |
|----------------------------------------------------------------|--|
| Organization Name*                                             |  |
| Primary Contact Name*                                          |  |
| Title/Role*                                                    |  |
| Email*                                                         |  |
| Phone                                                          |  |
| Legal Authority for Request (e.g., grant, contract, statute) * |  |

SECTION 2: PURPOSE, BENEFIT TO LLTC, & DATA USE

|                                                                                       |  |
|---------------------------------------------------------------------------------------|--|
| Purpose of Request* (describe what decision or research this data supports)           |  |
| Benefit to LLTC* (required for approval under Indigenous Data Sovereignty principles) |  |
| Intended Use (reports, analysis, research, evaluation, etc.) *                        |  |
| Deadline (YYYY-MM-DD) *                                                               |  |

SECTION 3: IRB STATUS (REQUIRED FOR ANY RESEARCH INVOLVING LLTC DATA)

|                              |  |
|------------------------------|--|
| IRB Status*                  |  |
| IRB Protocol (if applicable) |  |

SECTION 4: REQUESTED DATA ELEMENTS & FREQUENCY

|                                                                              |  |
|------------------------------------------------------------------------------|--|
| Specific Data Elements Requested* (list individually; attach spec if needed) |  |
| Timeframe/Cohort* (e.g., AY2024-25, FA2024)                                  |  |
| Frequency*                                                                   |  |

SECTION 5: DATA CLASSIFICATION, SECURITY, & PROTECTIONS

|                                                                                 |  |
|---------------------------------------------------------------------------------|--|
| Data Sensitivity Level*                                                         |  |
| Security Controls in Place* (storage, access, encryption, endpoint protections) |  |
| Transfer Method* (e.g., SFTP, encrypted SharePoint, secure vendor portal)       |  |
| Retention Period Requested*                                                     |  |

Destruction Plan\* (include method and certification timeline)

|  |
|--|
|  |
|--|

#### SECTION 6: PUBLICATION, ATTRIBUTION, & PRE-RELEASE REVIEW

Will findings be published or publicly shared? \*

|  |
|--|
|  |
|--|

Required Attribution / Citation Language (if known)

|  |
|--|
|  |
|--|

Is LLTC Pre-Publication Review Requested or Required? \*

|  |
|--|
|  |
|--|

#### SECTION 7: REQUIRED AGREEMENTS: MOA/DSA

Is an MOA/DSA in place? \*

|  |
|--|
|  |
|--|

If yes, list file name or describe terms

|  |
|--|
|  |
|--|

#### SECTION 8: CERTIFICATIONS

I certify that the requested data will be used only for the stated purpose and not redistributed.

Requestor Signature (full name) \*

|  |
|--|
|  |
|--|

**Appendix C: MOA/DSA Template (Key Clauses)**

**Leech Lake Tribal College: Memorandum of Agreement (MOA)**

**MEMORANDUM OF AGREEMENT (MOA)**

**For Data Access, Sharing, and Use**

This Memorandum of Agreement (MOA) is made and entered into by and between:

Leech Lake Tribal College (LLTC)

Address: 6945 Little Wolf Road NW, Cass Lake, MN 56633

**and**

[Partner Organization]

Address: \_\_\_\_\_

Effective Date: \_\_\_\_\_

End Date: \_\_\_\_\_ (or “Until completion of project and verified data destruction”)

**1. Purpose of Agreement**

This MOA establishes the terms under which LLTC will provide access to, or share, data with [Partner Organization], consistent with:

- LLTC Data Collection Policy: Internal & External Requests
- Indigenous Data Sovereignty principles
- FERPA and all applicable federal, state, and tribal requirements
- LLTC cultural protocols
- IRB review requirements (if applicable)

**The purpose of this data exchange is:**

[Describe purpose, decision supported, or research aims]

**Benefit to LLTC (required):**

[Describe how LLTC or community will benefit]

**2. Definitions**

- LLTC Data: Any information created, collected, stored, or maintained by LLTC.
- PII (Personally Identifiable Information): Information that may identify an individual directly or indirectly.
- Restricted Data: Sensitive information requiring the highest level of protection (e.g., SSNs, health data, tribal enrollment data).
- Confidential Data: Non-directory education records, HR data, course outcomes, financial records.

- De-identified Data: Data stripped of direct identifiers with reduced re-identification risk.

### 3. Scope of Data to Be Shared

LLTC agrees to provide the following data elements:

[List each element individually — minimum necessary only]

**Classification of data:**

- ☐ Restricted
- ☐ Confidential
- ☐ Internal
- ☐ Public

**Cohort / Timeframe:**

[Example: AY2024–25, FA2024]

**Frequency of Data Sharing:**

- ☐ One-time
- ☐ Monthly
- ☐ Quarterly
- ☐ Annual
- ☐ Other: \_\_\_\_\_

### 4. Permitted Uses and Limitations

**The data provided under this MOA:**

- May only be used for the purpose stated above
- May NOT be used for secondary analysis without additional LLTC approval
- May NOT be linked to other datasets without written approval
- May NOT be re-disclosed to any third parties
- May not be used to identify or stigmatize tribal communities or small-N groups
- Must reflect Indigenous Data Sovereignty: collective benefit, authority to control, responsibility, and ethics

**Any new use not explicitly stated in this MOA requires:**

1. A new external data request, and
2. An amendment to this MOA or a new agreement

### 5. Security Requirements

The receiving organization must implement the following safeguards:

- Encryption in transit and at rest

- Access is limited to named individuals only
- Secure device controls (password, endpoint protection)
- No storage in personal cloud accounts
- No emailing unencrypted files
- Physical and technical controls to prevent unauthorized use

**Storage Location:**

[Specify secure server, encrypted SharePoint/OneDrive, SFTP, etc.]

**6. IRB Requirements (If Applicable)**

If the purpose involves research with human participants or analysis that meets federal criteria for research:

- The external party must obtain IRB approval or exemption
- LLTC must receive IRB documentation before data is released
- Any participant consent materials must align with intended data use
- Secondary uses require additional IRB review

**IRB Determination:**

- ☐ Not applicable
- ☐ Exempt
- ☐ Approved — Protocol #: \_\_\_\_\_
- ☐ Pending (data cannot yet be shared)

**7. Indigenous Data Sovereignty & Cultural Protocols**

LLTC requires that all data uses comply with Indigenous Data Sovereignty principles:

- Community benefit
- Collective consent
- Transparency and accountability
- Respect for cultural protocols
- Shared interpretation of results when applicable
- LLTC right to review external publications prior to release

LLTC reserves the right to request removal of culturally inaccurate, harmful, or misrepresentative interpretations before publication.

## **8. Publication, Reporting, and Attribution**

**Will results be published or publicly shared?**

☐ Yes

☐ No

**If yes:**

- Publications must use only aggregated, suppressed, or de-identified data
- No cell sizes under 10 will be reported
- LLTC requires pre-publication review for accuracy and disclosure risk
- Required Attribution Language (if any):  
“Data provided by Leech Lake Tribal College (LLTC). Used with permission.”

## **9. Retention, Destruction, and Data Lifecycle**

Data may be retained only until:

Retention End Date: \_\_\_\_\_ (must be approved)

**Upon completion of the project or termination of this MOA, all LLTC data must be destroyed using approved methods:**

☐ Secure deletion

☐ Shredding (for physical materials)

☐ Verified purge of backups

☐ Other: \_\_\_\_\_

**A Destruction Certification must be submitted to LLTC within 30 days of destruction.**

## **10. Breach Notification**

The receiving organization must notify LLTC within 24 hours of any:

- Suspected or confirmed data breach
- Unauthorized access
- Loss or theft of devices containing LLTC data
- Any policy non-compliance

**LLTC reserves the right to suspend or terminate the agreement immediately in the event of a breach.**

## **11. Termination**

**This MOA may be terminated:**

- By either party with 30 days written notice

- Immediately by LLTC for any breach of terms
- Automatically upon project completion + verified data destruction

Upon termination, all data must be destroyed per Section 9.

## 12. Points of Contact

### LLTC DAIR (Primary Contact)

Name: \_\_\_\_\_

Email: \_\_\_\_\_

### Partner Organization Contact

Name: \_\_\_\_\_

Email: \_\_\_\_\_

## 13. Signatures

Leech Lake Tribal College (LLTC)

President or Authorized Administrator: \_\_\_\_\_

Date: \_\_\_\_\_

Director of Assessment & Institutional Research (DAIR): \_\_\_\_\_

Date: \_\_\_\_\_

Registrar (if student records involved): \_\_\_\_\_

Date: \_\_\_\_\_

IT/Security Officer: \_\_\_\_\_

Date: \_\_\_\_\_

Legal Counsel (if required): \_\_\_\_\_

Date: \_\_\_\_\_

For [Partner Organization]

Authorized Representative \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Leech Lake Tribal College: Data Sharing Agreement (DSA)**

**For Access, Sharing, Use, Protection, and Disposal of LLTC Data**

**This Data Sharing Agreement (DSA) is made and entered into by and between:**

Leech Lake Tribal College (LLTC)  
6945 Little Wolf Road NW  
Cass Lake, MN 56633

**and**

[Partner Organization]

Address: \_\_\_\_\_

Effective Date: \_\_\_\_\_

End Date: \_\_\_\_\_ (or “Until completion of project and verified data destruction”)

**1. Purpose of Agreement**

This DSA establishes the terms and conditions under which LLTC will disclose or exchange data with [Partner Organization], consistent with:

- LLTC Data Collection Policy: Internal & External Requests
- Indigenous Data Sovereignty principles
- FERPA, HIPAA/PHI (if applicable), GLBA, and all relevant federal, state, and tribal laws
- LLTC cultural protocols and privacy standards
- IRB review requirements (if research)

**Purpose of data access:**

|  |
|--|
|  |
|--|

**Benefit to LLTC (required):**

|  |
|--|
|  |
|--|

**2. Definitions**

- LLTC Data: Any information created, collected, generated, or maintained by LLTC.
- PII (Personally Identifiable Information): Any data that may identify an individual directly or indirectly.
- Restricted Data: Direct identifiers and highly sensitive information (e.g., SSN, tribal enrollment, health data).

- Confidential Data: FERPA-protected education records, HR records, advising notes, financial details.
- De-identified Data: Data stripped of direct identifiers and reduced in re-identification risk according to LLTC standards.
- Data Steward: LLTC functional owner responsible for data quality and access decisions.

### 3. Scope of Data Shared Under This Agreement

LLTC will provide the following data elements (minimum necessary only):

|  |
|--|
|  |
|--|

#### Data Classification:

- ☐ Restricted
- ☐ Confidential
- ☐ Internal
- ☐ Public

Timeframe / Cohort:

#### Frequency of Data Sharing:

- ☐ One-time
- ☐ Monthly
- ☐ Quarterly
- ☐ Annual
- ☐ Other: \_\_\_\_\_

Format:

- ☐ CSV
- ☐ Excel
- ☐ PDF
- ☐ De-identified Dataset
- ☐ Other: \_\_\_\_\_

### 4. Permitted Uses and Restrictions

The data may only be used for the purpose stated above.

It may not be used for any of the following without LLTC's written approval:

- Secondary analyses
- Linking or merging with other datasets
- Redisclosure to any third party

- Commercial, political, or predictive analytics unrelated to agreed purpose
- Identifying or stigmatizing Native communities, tribal citizens, or small-N groups
- Any use that conflicts with Indigenous Data Sovereignty values

**The recipient must:**

- Use data only for the stated purpose
- Store and handle data according to the protections listed in Section 6
- Notify LLTC if project scope or personnel change

**5. Indigenous Data Sovereignty Requirements**

LLTC requires that all external uses of LLTC data adhere to the following principles:

1. Collective Benefit: Data use must benefit LLTC, the Leech Lake Band of Ojibwe, or Native-serving communities.
2. Authority to Control: LLTC retains oversight of all uses of its data.
3. Responsibility: Data must be handled ethically, accurately, and in culturally respectful ways.
4. Ethics: Data must not cause harm, misrepresentation, or cultural disrespect.

**LLTC may require:**

- Co-interpretation of findings
- Review of cultural framing
- Reanalysis of whether results misrepresent LLTC or Native communities

**6. Security & Technical Safeguards**

The receiving organization must maintain administrative, physical, and technical safeguards including:

- Encryption in transit and at rest
- Access limitations to named personnel only
- Multi-factor authentication for systems containing LLTC data
- Endpoint protection on all devices accessing data
- Secure storage only:
  - ☐ SFTP
  - ☐ Encrypted SharePoint/OneDrive with restricted permissions
  - ☐ Approved vendor secure portal
  - Other (specify): \_\_\_\_\_

**Prohibited methods:**

- Unencrypted email
- Personal email or cloud storage
- USB drives without encryption
- Unsecured local devices

**7. IRB Approval (If Applicable)**

Research involving human participants or analyses that meet IRB criteria require:

- Approved IRB protocol or exemption before data release
- CITI training for involved researchers (if required by LLTC IRB or Data Governance Committee)
- Consent materials aligned with intended use

**IRB Status:**

- ☐ Not Applicable
- ☐ IRB Pending (data cannot be released)
- ☐ IRB Approved
- ☐ IRB Exempt

**8. Publication, Disclosure, and Reporting**

If results are published or shared publicly:

- All reported values must meet LLTC suppression rules (no cell < 10).
- Only aggregated, de-identified information may be published.
- No tribal enrollment info, small-N programs, or culturally sensitive areas may be disclosed.
- LLTC requires pre-publication review for accuracy and cultural integrity.

**Attribution language (required):**

“Data provided by Leech Lake Tribal College (LLTC). Used with permission.”

Recipient agrees to provide LLTC:

- Draft publications or reports at least 30 days before release
- Final copies of publications

**9. Data Retention & Destruction**

Data may be retained only until:

Retention End Date: \_\_\_\_\_

**Upon expiration of this agreement, all LLTC data must be destroyed via:**

- ☐ Secure deletion
- ☐ Shredding of physical materials
- ☐ Verified purge of backups
- ☐ Other: \_\_\_\_\_

A Data Destruction Certification must be submitted to LLTC within 30 days of project completion or termination.

#### **10. Breach, Incident Response, & Notification**

Recipient must notify LLTC within 24 hours of any:

- Suspected or confirmed data breach
- Unauthorized access
- Compromise of systems or credentials
- Non-compliance with this DSA

LLTC may immediately suspend data access or terminate the agreement in response to breaches.

#### **11. Termination**

This DSA may be terminated:

- By either party with 30-day written notice
- Immediately by LLTC for any breach
- Automatically upon project completion and data destruction verification

**Upon termination, all conditions of Section 9 must be fulfilled.**

#### **12. Points of Contact**

LLTC Primary Contact (DAIR):

Name: \_\_\_\_\_

Email: \_\_\_\_\_

Phone: \_\_\_\_\_

Partner Organization Contact:

Name: \_\_\_\_\_

Email: \_\_\_\_\_

Phone: \_\_\_\_\_

#### **13. Signatures**

For Leech Lake Tribal College (LLTC):

Authorized Administrator: \_\_\_\_\_

Date: \_\_\_\_\_

Director of Assessment & Institutional Research (DAIR): \_\_\_\_\_

Date: \_\_\_\_\_

Registrar (if student records involved): \_\_\_\_\_

Date: \_\_\_\_\_

IT/Security Officer: \_\_\_\_\_

Date: \_\_\_\_\_

Legal Counsel (if required): \_\_\_\_\_

Date: \_\_\_\_\_

For [Partner Organization]: \_\_\_\_\_

Authorized Representative: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## **Appendix D: Disclosure Risk & Suppression Standards**

### **Leech Lake Tribal College (LLTC)**

#### **Data Collection Policy: Internal & External Requests**

LLTC is committed to protecting the privacy of students, employees, and community members, as well as upholding Indigenous Data Sovereignty principles. To prevent unintended disclosure or re-identification of individuals or small groups, especially in tribal, rural, or small-number (small-N) educational contexts, LLTC applies the following disclosure risk mitigation and suppression standards to all public-facing reports, dashboards, research outputs, and external data releases.

#### **1. Minimum Cell Size Rule (Primary Suppression)**

- No publicly released table, chart, narrative, or statistics may display a cell size less than 10.
- This includes:
  - Headcount
  - Subgroup counts (e.g., age ranges, gender, program-level)
  - Outcome rates (e.g., retention, completion, course success)
  - Any disaggregated or cross-tabulated data
- Cells below 10 must be:
  - Suppressed,
  - Combined with other categories, or
  - Reported as “<10” without specifying the exact value.

#### **2. Complementary (Secondary) Suppression**

When primary suppression (e.g., hiding values <10) would allow remaining cells to be used to infer those suppressed numbers:

- Additional (“complementary”) cells must also be suppressed to prevent reverse calculation.
- This includes:
  - Totals, if they reveal a suppressed subgroup
  - Opposite-category cells that would allow back-calculation
  - Small-N categories that become identifiable after row/column deduction  
\*\*(where “N” Represents the sample size) refers to studies that focus on a limited number of participants, where Large-N studies use group averages to find trends).

LLTC analysts will apply complementary suppression as needed to ensure no suppressed value can be inferred.

#### **3. Small-N Program, Cohort, and Subgroup Protection**

Because LLTC serves small and tightly connected communities, the following also apply:

- Programs, departments, or cohorts with fewer than 20 individuals may be aggregated into:
  - “Other Programs”
  - “Combined STEM”
  - “Combined General Education”
  - A broader academic or service category
- Academic programs with fewer than 10 graduates in a multi-year period may be:
  - Reported only in multi-year aggregates, or
  - Suppressed from external publications entirely

LLTC reserves the right to withhold or aggregate data when subgroup disclosure could pose cultural, community, or reputational risk.

#### **4. Percentage and Rate Suppression**

- Percentages based on denominators under 20 may not be reported publicly.
- Percentages corresponding to suppressed numerical values must also be suppressed.
- Any rate that could enable re-identification (e.g., “67% of 6 students”) will be removed or replaced with:
  - “Rate suppressed due to small-N,” or
  - A broader aggregated statistic.

#### **5. Rounding and Blurring Techniques**

To further reduce re-identification risk:

- Percentages are rounded to one decimal place.
- Extremely high or low outcomes (example: 100%, 0%) for small groups may be:
  - Reported as a range (example: “≥95%”),
  - Suppressed entirely, or
  - Aggregated into a multi-cohort summary.

Analysts may apply top-coding (e.g., “10+ years,” “5+ attempts”) or bottom-coding where needed.

#### **6. De-identification Requirements**

Before any dataset leaves LLTC (internally or externally), the following must be removed unless explicitly approved under MOA/DSA and FERPA exceptions:

- Names, ID numbers, SSNs

- Full dates of birth (use year or age range only)
- Addresses, phone numbers, personal email
- Tribal enrollment numbers or documentation
- Health or disability information (unless authorized under IRB-approved protocols)
- Advisor notes, case-management data, or other sensitive notes

Indirect identifiers must also be evaluated for risk, particularly in combination (e.g., major, age, hometown, gender).

## **7. High-Risk Variables**

The following require elevated scrutiny due to their potential to identify individuals in small tribal communities:

- Tribal enrollment or citizenship
- Indigenous language proficiency
- Employment at LLTC
- Internship/placement sites in local organizations
- Rare academic programs or certifications
- First-generation status combined with other identifiers
- Disability accommodation data
- Small course sections (where data is less than 10 students)

These may only be reported in aggregated or multi-year form.

## **8. Geographic Privacy Protection**

- Home communities, reservation districts, census blocks, or tribal housing locations may not be reported unless population sampled is greater than 20.
- Zip codes with small populations may require aggregation into:
  - Regional groupings
  - Tribal areas vs. non-tribal areas
  - Northern/central/southern county groupings

## **9. Narrative and Qualitative Data Protection**

For qualitative results (e.g., surveys, interviews, focus groups):

- Quotes must be anonymized and scrubbed out of identifiable details.
- If a participant describes a unique event or role that could reveal identity, LLTC may:

- Paraphrase,
- Aggregate themes, or
- Withhold the content entirely.

Indigenous community stories or cultural references must be reviewed for cultural sensitivity and community impact.

#### **10. External Publications & Review**

All external reports, publications, or presentations using LLTC data must:

1. Adhere to these suppression standards
2. Undergo pre-publication review by LLTC DAIR
3. Reflect Indigenous Data Sovereignty principles, including benefit to the community

Public release is prohibited if re-identification risk cannot be mitigated.

#### **11. Exceptions and Special Cases**

Exceptions may be granted only when:

- Required by federal reporting (IPEDS, Title III/IV, grant obligations)
- Approved by the Director of Assessment & Institutional Research
- Approved by the Data Governance Committee
- Approved by the Registrar (if student-level FERPA data involved)
- Included explicitly in an MOA/DSA
- Permitted under an IRB-approved protocol

Even in such cases, LLTC retains the authority to limit or condition release to protect community privacy.

## **Appendix E: Definitions Specific to this Policy**

### **Academic Data**

Information related to student coursework, grades, academic progress, enrollment, program participation, and related academic performance metrics.

### **Aggregated Data**

Data that has been combined into summary statistics (e.g., totals, averages, rates) so that no individual-level data can be reasonably identified.

### **Confidential Data**

Sensitive LLTC data that is not publicly available and requires restricted access, including non-directory student education records protected under FERPA, HR personnel data, advising or case-management notes, and detailed financial or academic performance information.

### **Data Custodian**

A staff member or unit responsible for maintaining the systems where LLTC data resides (e.g., IT, Registrar). Custodians provide system access but do not authorize data release.

### **Data Steward**

A functional owner responsible for the quality, definitions, and approval of access or release for a specific data domain (e.g., Registrar for student data, Finance for financial data).

### **Data Subject**

The individual or group about whom the data is collected (e.g., students, employees, applicants, community members).

### **De-identified Data**

Data that has had all direct identifiers removed, with indirect identifiers sufficiently minimized or altered to reduce re-identification risk to a very low level. De-identified data still carries disclosure risk if the sample is small.

### **Direct Identifier**

Information that directly identifies an individual, such as name, SSN, full date of birth, student ID, phone number, mailing address, tribal enrollment number, or personal email.

### **Disclosure Risk**

The likelihood that data alone or in combination with other data could identify an individual, small subgroup, or culturally specific population.

### **External Data Request**

Any request for LLTC data submitted by entities outside LLTC (e.g., researchers, vendors, funders, institutions, agencies). External requests require approval per the policy and may require an MOA/DSA and IRB review.

### **FERPA (Family Educational Rights and Privacy Act)**

Federal legislation protecting the privacy of student education records. FERPA governs access, disclosure, consent, and rights related to student information.

### **Highly Sensitive / Restricted Data**

The most sensitive LLTC data requiring the highest level of protection, including direct identifiers, health or disability information, tribal enrollment or citizenship information, authentication credentials, financial account numbers, or legally protected categories of data.

### **Indigenous Data Sovereignty**

The right of Indigenous Peoples to manage, control, and govern the collection, access, interpretation, stewardship, and application of data about their peoples, cultures, lands, and institutions. Principles include collective benefit, authority to control, responsibility, and ethics.

### **Institutional Data Governance Committee (DGC)**

The LLTC committee responsible for interpreting data governance policies, resolving escalated requests, approving high-risk data releases, and maintaining data standards and classification frameworks.

### **Internal Data Request**

A request submitted by LLTC personnel for institutional operations, reporting, assessment, accreditation, planning, compliance, or program improvement.

### **IRB (Institutional Review Board)**

The body responsible for reviewing research involving human participants to ensure ethical protections, informed consent, privacy, and compliance with regulatory standards.

### **Memorandum of Agreement (MOA)**

A formal agreement governing ongoing or significant data exchange between LLTC and another organization. Specifies purpose, scope, data elements, safeguards, permitted uses, restrictions, retention, and destruction requirements.

### **Data Sharing Agreement (DSA)**

A legally binding document that specifies how LLTC data may be accessed, shared, stored, protected, used, retained, and destroyed by an external entity. DSAs are required for any sharing involving PII, PHI, or sensitive data.

### **Minimum Necessary Principle**

A privacy rule requiring that only the smallest amount of data necessary to fulfill a legitimate purpose be collected, used, accessed, or disclosed.

### **Personally Identifiable Information (PII)**

Information that can identify an individual directly or indirectly, including combinations of indirect identifiers (e.g., major + age + hometown + gender).

### **Public Data**

Information that LLTC has intentionally made public, such as factbooks, institutional statistics, approved reports, accreditation summaries, or policy documents.

### **Re-identification**

The process by which an individual can be identified from anonymized or de-identified data through linkage, inference, or small-N analysis.

### **Small-N Data**

Data describing groups is so small that identity may be inferred (typically fewer than 10 individuals), even when direct identifiers are removed.

### **Suppression**

The removal or hiding of data values to reduce disclosure risk, particularly when cell counts fall below LLTC's minimum cell size rule.

### **Vendor**

An external organization that provides a system, platform, tool, or service requiring LLTC data. Vendor access requires a security review and a DSA or contract specifying data protections.