SECTION #: 1.0 General

SUBJECT: AI Usage and Guidelines

Background: Artificial intelligence and large language model (LLM) technologies are rapidly transforming how organizations operate, communicate, and make decisions. As these tools become increasingly accessible and integrated into everyday workflows, LC State is committed to enabling their responsible use in a manner that supports institutional effectiveness while safeguarding the privacy, security, and rights of students, employees, and the broader campus community. This policy provides the framework necessary to realize the benefits of AI tools while managing associated risks.

Point of Contact: Chief Information Officer, Office of Information Technology Services

Other LC State offices directly involved with implementation of this policy, or significantly affected by the policy: Human Resources

Date of approval by LC State authority: May, 2026

Date of State Board Approval: N/A

Date of Most Recent Review: New Policy

Summary of Major Changes incorporated in this revision to the policy: New policy.

---

1. Purpose and Scope

Lewis-Clark State College (LC State) recognizes that faculty and staff may seek to use generative artificial intelligence (AI) platforms, including large language model (LLM) platforms, to conduct institutional business or perform work-related tasks. This policy establishes guidelines for the appropriate, secure, and responsible use of AI tools while protecting institutional data and ensuring compliance with applicable laws and regulations.

A. Policy Scope

This policy applies to LC State faculty and staff who use AI/LLM platforms for administrative purposes on behalf of the institution. This includes full-time and part-time employees, contractors, consultants, and temporary personnel who access LC State systems or handle institutional data.

This policy does not govern academic uses of AI in teaching and learning contexts, which may be addressed through separate academic policies.

This standard does not supersede any other applicable law or stricter agency directive or existing labor management agreement in effect as of the effective date of this policy.

ITS reserves the right to revoke, change, or supplement this document at any time without prior notice. Such changes must be effective immediately upon approval by management, unless otherwise stated.

2. Definitions

Artificial Intelligence (AI): Broadly defined as technology that produces new text, images, audio, code, and other content based on training data and user inputs. AI includes but is not limited to LLM platforms, image generators, code assistants, and other software tools that incorporate generative AI elements. Some software uses AI to suggest changes, summarize information, translate text, or analyze data.

Large Language Model (LLM): AI systems specifically designed to understand and generate human language, such as ChatGPT, Claude, and similar conversational AI platforms. Approved AI tools must be accessed through LC State-managed licenses that authenticate via the institution's Single Sign-On (SSO) system.

3. Risks and Considerations

AI technology presents unique risks that all users must understand:

A. Accuracy and Reliability

AI systems can produce inaccurate, erroneous, incomplete, or fabricated output. This phenomenon, often called "hallucination," means AI-generated content can be difficult to distinguish from reliable work product without verification through traditional means. This verification can be impractical when voluminous data must be analyzed or significant time or expense would be required.

B. Intellectual Property Concerns

Users must be mindful of potential infringements on copyrights, trademarks, patents, or other legal protections that may arise from input provided to or output generated by AI tools. AI-generated content may:

- Be subject to the bias of its creators
- Contain information with copyright concerns
- Include plagiarized content
- Raise other intellectual property concerns

C. Data Privacy and Security

AI platforms operate on external servers beyond LC State's direct control. Information entered into these systems may be used to train future models, stored on third-party infrastructure, or otherwise processed in ways that compromise data security and institutional privacy.

D. FERPA Compliance

The Family Educational Rights and Privacy Act (FERPA) strictly regulates the disclosure of student education records. AI systems are considered third parties under FERPA, and inputting student information into AI tools without proper safeguards such as obfuscation, including masking or redaction, constitutes an unauthorized disclosure of education records.

4. Approved AI Tools and Access Requirements

A. Centralized License Management

All use of AI/LLM platforms for LC State business must be conducted through licenses centrally managed by the Office of Information Technology Services (ITS). Users must authenticate through LC State's Single Sign-On (SSO) system to access approved tools.

B. Currently Approved Platforms

The following AI platforms are currently approved for use:

- Claude (Anthropic)
- ChatGPT (OpenAI)
- Microsoft Copilot

C. Requesting Access

Faculty and staff who require access to approved AI tools must:

- Submit a request through ITS following the standard software approval process
- Demonstrate a legitimate business need for the requested tool
- Complete required training before access is granted (see Section 9)
- Acknowledge understanding of and agreement to comply with this policy

D. Requesting Additional AI Tools

Requests for AI tools not currently approved must follow LC State's Vendor Management Policy. The approval process by ITS includes:

- Submission of a formal request
- Vendor security and privacy review conducted
- Assessment of data handling practices and compliance with institutional policies
- Evaluation of licensing terms and data residency requirements
- Written approval from the ITS Department before any use

No employee may use any AI/LLM platform for institutional business without prior written approval from ITS.

5. Data Classification and Permissible Use

All AI tool usage must comply with the LC State Data Use Guidelines. Users must understand and apply the institution's data classification framework when determining what information may be entered into AI systems. https://www.lcsc.edu/it/data-classification-and-labeling

A. Prohibited Data - Never Permitted in AI Tools

The following data classifications are strictly prohibited from being entered into any AI/LLM platform:

- Restricted Data
- Confidential Data

B. Internal Data may be entered into AI tools only with explicit consideration of the following factors:

- The specific business need for using AI with this data
- Whether the data contains proprietary information that could harm LC State if disclosed
- The sensitivity of planning documents or strategic information
- Potential exposure of business partner information

When Microsoft Copilot is configured with appropriate Purview data loss prevention controls, Internal Data classified and protected through these systems may be processed by Copilot within those controlled environments.

Users must exercise judgment and consult with their supervisor or ITS when uncertain whether Internal Data is appropriate for AI processing.

C. Public Data - Generally Permitted

Public Data may be entered into approved AI tools accessed through LC State SSO-managed licenses. This includes:

- Staff directory information
- Department names and contact information
- Course descriptions and schedules
- LC State calendar dates
- Campus maps
- Publicly reported summary statistics
- Other information approved for unrestricted distribution

D. Employee Personal Information

No employee personal information may be entered into AI/LLM platforms unless it is already classified as Public Data.

E. Microsoft Copilot and Purview Integration

LC State has implemented Microsoft Purview to classify and protect institutional data within the Microsoft 365 environment. These include:

- Copilot access to Teams, SharePoint, and OneDrive content will be restricted based on data classification labels

- Documents classified as Confidential or Restricted will be excluded from Copilot scanning
- Users must ensure Purview classifications are applied correctly to their documents

Copilot may process Internal and Public data within the M365 environment according to configured data governance policies

6. Required Best Practices and User Responsibilities

All users of approved AI tools must comply with the following practices:

A. Critical Evaluation of Output

Users must critically evaluate all output from AI/LLM platforms before using it for institutional purposes. AI-generated content must never be accepted at face value. Users must:

- Verify factual claims through authoritative sources
- Check for logical inconsistencies or errors
- Validate any data, statistics, or references provided
- Review content for potential bias or inappropriate material
- Ensure citations and sources actually exist and support the claims made

B. Human Review and Validation

AI output must not be used to make institutional decisions or produce deliverables without proper human review. This is particularly critical for:

- Communications to students, parents, or external stakeholders
- Financial or budget-related decisions
- Policy recommendations
- Legal or compliance matters
- Personnel decisions

C. Transparency and Attribution

When AI tools substantially contribute to work products, users should:

- Disclose the use of AI assistance where appropriate
- Take responsibility for the final work product
- Ensure the output meets institutional quality standards
- Not misrepresent AI-generated content as solely human-created when accuracy or authenticity matters

D. Human Oversight Requirements for High-Stakes Decisions

LC State recognizes that certain decisions carry significant consequences for individuals and the institution. AI must augment, not replace, human judgment in these contexts.

i. Definition of High-Stakes Decisions

High-stakes decisions are those that directly and materially affect: student outcomes (admissions, financial aid, academic standing, graduation eligibility, disciplinary actions); employment matters (hiring, promotion, compensation, performance evaluation, discipline, or termination); financial impacts (budget allocations, expenditure approvals, contracts, or financial obligations exceeding departmental thresholds); legal or compliance obligations; institutional reputation; or health and safety.

ii. Mandatory Human Review Requirements

For all high-stakes decisions:

- AI must be assistive only - AI may inform, suggest, or provide analysis; AI may NOT make or automate final decisions; a qualified human decision-maker must review, evaluate, and approve all AI inputs
- Documented decision authority - the human decision-maker must be clearly identified with appropriate expertise and authority
- Independent evaluation - decision-maker must critically evaluate AI recommendations and be empowered to override or disregard AI suggestions
- Decision documentation - record how AI was used, document the human decision-maker's evaluation and reasoning, note any instances where AI recommendations were modified or rejected
- No automation of high-stakes decisions - each case must receive individual human consideration with explicit human approval checkpoints

iii. Examples of Required Human Oversight

Permitted: Using AI to summarize student applications for human review; AI-generated analysis of employment candidate qualifications with hiring committee making final decisions; AI-assisted financial forecasting to inform budget planning; AI draft communications reviewed and approved before sending.

Prohibited: Automated rejection of student applications based on AI scoring; AI-determined salary increases or job classifications without human review; automated financial aid awards based solely on AI calculations; auto-generated external communications sent without human review.

iv. Right to Human Review

Any individual adversely affected by an AI-influenced decision has the right to know that AI was used in the decision process and to request a review by a human decision-maker who will consider the case independently, explain the basis for the decision, and have authority to modify or reverse the decision if warranted. Requests should be submitted to the office or department that made the original decision.

E. Appropriate Use Authorization

Users must use approved AI platforms solely for work-related purposes; access tools only through LC State SSO-managed licenses; use AI in a manner compliant with the authorization granted by ITS; not share login credentials or access methods with unauthorized individuals; and not attempt to circumvent technical or policy controls.

F. Device and Platform Compliance

This policy applies to the use of AI tools on any device, whether LC State-owned or personal, when conducting institutional business. Users accessing approved AI platforms from personal devices must still authenticate through LC State SSO, comply with all data classification and usage restrictions, understand that institutional monitoring may apply to business use, and take appropriate security precautions to protect institutional data.

7. Prohibited Uses

The following uses of AI tools are strictly prohibited:

A. Unauthorized Data Disclosure

- Entering any Restricted or Confidential data into AI platforms
- Sharing proprietary LC State information not available to the public
- Disclosing information that could compromise institutional security
- Processing personal information of students, employees, or other individuals in violation of privacy laws

B. Unauthorized Platform Use

- Using AI platforms not approved by ITS
- Accessing approved platforms through personal accounts rather than LC State SSO
- Sharing institutional login credentials with others
- Using AI tools before receiving required training and authorization

C. Inappropriate Content Generation

- Creating content that violates LC State policies on discrimination, harassment, or appropriate conduct
- Generating misleading or deceptive communications
- Producing content that misrepresents the institution's positions or policies

D. Academic Integrity Violations

- Using AI to complete work that should represent individual effort and expertise
- Misrepresenting AI-generated content as original work when such representation matters

8. Training Requirements

A. Mandatory Training

Before being granted access to approved AI tools, users must complete training that covers:

- Understanding AI capabilities and limitations
- Data classification and what information may be entered into AI systems
- FERPA compliance and student data protection
- Critical evaluation of AI output

- Appropriate use cases and prohibited practices
- Incident reporting procedures

B. Training Delivery

Training will be developed and delivered by ITS in coordination with relevant campus stakeholders. Training may be delivered through online modules, in-person or virtual sessions, documentation and self-study materials, and department-specific training for high-use areas.

C. Ongoing Education

ITS will provide periodic updates and refresher training as new AI tools are approved, policies or best practices evolve, significant security incidents or concerns emerge, or technology capabilities change substantially.

9. AI System Inventory and Monitoring

A. Institutional AI Inventory

ITS shall maintain a comprehensive inventory of all approved AI systems and applications in use across LC State. This inventory ensures accountability, enables effective governance, and supports institutional planning. The inventory will track tool/platform name, vendor/provider, departments using the tool, primary use cases, governance tier, data classification level, authorization date, authorized users, review date, and status.

ITS will update the inventory monthly or as changes occur. Departments must notify ITS of changes in use cases or scope within 10 business days. An annual comprehensive inventory validation will be conducted each academic year, and a summary inventory report will be provided to senior leadership quarterly.

B. Continuous Monitoring and Evaluation

LC State is committed to ongoing monitoring of AI systems to ensure they deliver value, maintain security, and operate within approved parameters. ITS will monitor AI tool usage through access logs, volume metrics, user activity tracking, and anomaly detection.

All AI applications must undergo periodic effectiveness reviews based on governance tier. Tier 1 applications receive annual departmental self-assessment; Tier 2 receive semi-annual effectiveness review; Tier 3 receive quarterly monitoring reports and semi-annual comprehensive evaluation including outcome metrics, bias and fairness assessment, security and compliance review, and cost-benefit validation.

C. Continuous Improvement Process

ITS will maintain a lessons-learned repository documenting successful use cases and best practices, challenges encountered and solutions, policy clarifications needed, training gaps identified, and technology limitations discovered. Multiple feedback channels will be maintained including formal effectiveness reviews, user surveys, incident reports, consultation sessions, and annual policy review.

D. Reporting and Transparency

ITS will provide regular reports to department leadership, senior leadership, governance committees, and Faculty Senate (as appropriate). Consistent with Idaho's framework emphasis on transparency, LC State will maintain a public-facing summary of approved AI tools, disclose AI use in high-stakes external-facing applications, and report AI governance approach in institutional accountability documents.

10. Incident Reporting

Users must immediately report any of the following to ITS:

- Suspected or confirmed unauthorized disclosure of institutional data to AI platforms
- Accidental entry of Restricted or Confidential data into AI systems
- AI-generated content that raises concerns about accuracy, bias, or appropriateness
- Security concerns related to AI platform access or use
- Observed policy violations by other users

Reports should be submitted to ITS: Email: helpdesk@lcsc.edu | Phone: 208-792-2231

All incidents will be reviewed in accordance with LC State's Incident Response Procedures.

11. Risk-Based Governance Framework

LC State employs a risk-based approach to AI governance that ensures oversight is proportionate to the potential impact of each AI application. This framework enables innovation for low-risk use cases while providing rigorous oversight for high-stakes applications.

A. Risk Assessment Model

All AI use cases must be evaluated using the following six risk factors:

i. Data Sensitivity

- Low Risk: Public data only
- Moderate Risk: Internal data with limited sensitivity
- High Risk: Confidential or Restricted data (requires explicit exception approval from the ITS department)

ii. Decision Impact

- Low Risk: Informational only, no direct impact on individuals or operations
- Moderate Risk: Affects departmental operations or resource allocation
- High Risk: Directly affects individual rights, opportunities, safety, or institutional compliance obligations

iii. Autonomy Level

- Low Risk: Purely assistive, all outputs reviewed by humans before use
- Moderate Risk: Semi-autonomous with human oversight at key decision points
- High Risk: Autonomous or automated decision-making with limited human intervention

iv. Transparency

- Low Risk: Clear, explainable outputs with visible reasoning
- Moderate Risk: Some opacity in processing but outcomes can be validated
- High Risk: "Black box" systems where reasoning is difficult to trace or explain

v. Scope and Scale

- Low Risk: Individual or small team use (1-10 people)
- Moderate Risk: Departmental use (10-50 people) or multiple departments
- High Risk: Institution-wide deployment (50+ people) or external-facing applications

vi. Novelty and Complexity

- Low Risk: Well-established use case with proven track record
- Moderate Risk: Emerging application with some organizational precedent
- High Risk: Novel application without established best practices or significant technical complexity

B. Governance Tiers

Based on the risk assessment, AI applications are assigned to one of three governance tiers:

i. Tier 1: Low-Risk Applications

Characteristics: Uses Public data only; purely informational or assistive; affects individual users or small teams; well-established use cases; full human review of all outputs before use.

Examples: Drafting routine email responses; summarizing public documents; brainstorming ideas or generating outlines; grammar and writing assistance; translating public content.

Governance Requirements: Standard approval through ITS software request process; completion of required training; compliance with general best practices (Section 7); annual usage review by department.

Review Process: Lightweight technical review by ITS (5-10 business days).

ii. Tier 2: Moderate-Risk Applications

Characteristics: May process Internal data; influences but does not determine decisions; affects departmental operations; moderate scale deployment; human oversight at key points.

Examples: Analyzing trends in operational data for planning purposes; generating draft reports that will be thoroughly reviewed; assisting with budget analysis or forecasting; supporting recruitment or admissions processes (with human decision-making); creating training materials or educational content.

Governance Requirements: Formal business justification and expected outcomes documentation; risk assessment completed by requesting department; technical and security review by ITS; data classification verification; enhanced monitoring and periodic effectiveness review; documented human oversight protocols.

Review Process: Technical and ethical consultation by ITS and relevant stakeholders (15-20 business days).

iii. Tier 3: High-Risk Applications

Characteristics: Processes Confidential or Restricted data (requires exception); directly influences high-stakes decisions; affects individual rights, opportunities, or safety; institution-wide or external-facing deployment; novel or complex applications.

Examples: AI systems that influence student admissions decisions; tools that inform employment or promotion decisions; automated financial aid calculations or determinations; systems processing student educational records; external-facing chatbots representing the institution; predictive models for student success or retention.

Governance Requirements: Comprehensive business case; full risk assessment with mitigation strategies; multi-stakeholder review including ITS, Legal, Data Governance Committee, and Ethics consultation; senior leadership approval; mandatory human oversight; continuous monitoring; regular audit and effectiveness reviews (at least annually); documented explainability and appeals process; public disclosure of AI use where appropriate.

Review Process: Full multi-body oversight (30-45 business days minimum).

C. Risk Assessment Process

When requesting access to new AI tools or implementing new AI applications, departments must:

- Complete Risk Assessment Form - Available from ITS, documenting all six risk factors
- Identify Governance Tier - Self-assess which tier applies based on risk factors
- Submit Request - Include risk assessment with access request or implementation proposal
- ITS Validation - ITS reviews and confirms or adjusts tier assignment
- Follow Tier-Specific Process - Complete requirements for assigned governance tier

D. Escalation and Reclassification

AI applications may be reclassified to a higher governance tier if the scope of use expands beyond original approval, new risk factors emerge during deployment, data classification of processed information changes, incidents or concerns arise during use, or technology capabilities evolve in ways that increase risk. ITS reserves the right to reclassify applications and require compliance with higher tier requirements at any time.

12. Enforcement and Accountability

A. Policy Violations

Failure to comply with this policy may result in immediate revocation of access to AI tools; temporary or permanent restrictions on access to other LC State systems and services; disciplinary action in accordance with institutional policies and employment contracts; and legal consequences if violations involve breach of law or regulation.

B. Determining Appropriate Action

The severity of consequences will be determined based on the nature and extent of the policy violation, whether the violation was inadvertent or intentional, the sensitivity of data involved, whether harm resulted to individuals or the institution, the user's history of compliance, and other relevant factors.

C. Reporting Structure

Policy violations and resulting actions will be coordinated between the Office of Information Technology Services, Human Resources, the violator's supervisor and department head, and other offices as appropriate to the nature of the violation.

13. Questions and Guidance

Questions about this policy should be directed to the Office of Information Technology Services (ITS):
Email: helpdesk@lcsc.edu | Phone: 208-792-2231

For data classification questions, also refer to the LC State Data Use Guidelines and ITS Data Governance resources.

14. Related Policies and Resources

This policy should be read in conjunction with:

- LC State Data Use Guidelines
- Vendor Management Policy
- Acceptable Use Policy
- FERPA Compliance Procedures
- Incident Response Procedures
- Information Security Policies