Missouri Western State University

Policy Name: Artificial Intelligence (AI) Usage and Governance	**Responsible Office**: Technology Services
Policy Category: Compliance and Governance	**Approving Authority**: Vice President for Finance and Administration
Date Effective: July 1, 2026	**Date Last Reviewed/Revised:** October 14, 2026

I. Purpose

This policy establishes expectations for the safe, ethical, and secure use of AI and large-language-model (LLM) applications to protect institutional data, privacy, intellectual property, accessibility, and academic integrity. Of the many risks associated with the use of AI tools and applications, among the most significant is ensuring appropriate use of Missouri Western data.

II. Applicability

This policy applies to all University employees, student workers, graduate assistants, contractors, and affiliates using AI services through University-managed systems, including Google Workspace for Education (e.g., Gemini for Education, NotebookLM), and any current or future authorized AI platforms (e.g., Microsoft Copilot, Anthropic Claude, OpenAI ChatGPT Enterprise). It also extends to partnerships and collaborations involving AI within and beyond Missouri Western.

III. Definitions

AI Disclosure. The process of acknowledging when AI significantly contributed to an official document or communication.

AI Tool. A general term identifying applications, services, features, and add-ins that leverage AI to create content or otherwise support or enhance the creation of content, whether as a stand-alone application or service or as functionality embedded within another tool, platform, or service.

Artificial Intelligence (AI). Systems or tools that perform tasks typically requiring human intelligence, including machine learning and LLMs such as ChatGPT or Microsoft Copilot.

Authorized AI System. A University-licensed, procured, managed, and authorized AI Tool integrated into MWSU systems and authorized by the University for institutional use. These tools have been assessed by Technology Services and have undergone review for contractual protections, security requirements, and applicable privacy and data use terms intended to protect University data and other information used with the tools.

Regulated Data. Regulated Data includes Restricted, Confidential, and Controlled Internal Institutional Dat and/or sensitive data that could cause legal, financial, reputational, or operational harm to Missouri Western and/or its community members if disclosed or could require compliance efforts if exposed to unauthorized parties.

High-Impact Decision. An AI-assisted or automated decision that could materially affect individuals or the institution (e.g., hiring, admissions, discipline, or financial aid).

Publicly Available AI Systems: AI tools that are accessible to the general public via the internet, without University vetting, procurement, or approval.

IV. Policy

Missouri Western State University recognizes the transformative potential of Artificial Intelligence (AI) technologies to improve efficiency, insight, and decision-making across university operations. While the use of AI Tools creates new opportunities for the University community, that same usage can present substantial legal, regulatory, and reputational risks that MWSU must balance. Decisions affecting University operations, academic matters, employment actions, admissions, student outcomes, research conclusions, healthcare activities, or legal obligations may not rely solely on AI-generated outputs and require appropriate human review and judgment. Individuals remain responsible for all actions taken by AI Tools and systems operating on their behalf and must ensure outputs and actions are reviewed for accuracy, appropriateness, and compliance with University policy.

AI use must safeguard personal and institutional information and comply with applicable privacy, security, and data protection standards, especially for high-risk or sensitive data. All community members are expected to protect personal and confidential information when using AI tools and use AI in a manner that respect human dignity, fairness, and social responsibility.

Compliance with this policy does not relieve an individual from their responsibility to comply will other applicable policies, including, but not limited to the Data Governance, Classification, and Acceptable Use, Intellectual Property, Faculty Handbook, Student Code of Conduct, University research policies, and policies and guidance issued by Technology Services.

V. Procedures and Implementation

A. Responsible and Ethical Use

1. Responsible and Ethical Use

MWSU encourages the use of AI to enhance productivity and clarity while maintaining human oversight. Users must:

a) Review outputs for accuracy, bias, and fairness.
b) Maintain human-centered judgment; AI may assist but not replace human decision-making.

c) Ensure transparency and disclose AI assistance when AI meaningfully contributes to official work products, consistent with the AI Use Disclosure Guidance (Appendix C).
d) Protect privacy and intellectual integrity; do not fabricate data, impersonate others, or misrepresent authorship.
e) Remain personally responsible for all content produced or assisted by AI, including verifying accuracy, appropriateness, and compliance with University policies and applicable laws.

B. Acceptable and Prohibited Use - Handling Requirements

Use of AI tools must comply with the University's data classification as set forth in the Data Governance, Classification, and Acceptable Use policy and any issued guidance documents. Restricted, Confidential, and Controlled Internal Data are prohibited in Publicly Available AI Systems.

Restricted, Confidential, and Controlled Internal Institutional Data and may only be used in Authorized AI Systems with appropriate safeguards and when formally authorized by the Information Security Officer (ISO) or designee and subject to a Data Protection Addendum (DPA) and security controls.

AI-generated outputs must be reviewed by the responsible employee or decision-maker prior to publication, dissemination, or reliance in official actions. The level of review should be appropriate to the risk and context of the use.

Users must ensure that AI-generated content incorporated into official University documents complies with applicable copyright and intellectual property requirements. Transparency is required when AI meaningfully contributes to substantive content, analysis, or conclusions.

Personal experimentation with Publicly Available AI Systems must not involve University data or credentials.

Institutional Data classification requirements and applicable privacy laws remain in effect. Rule of thumb: If the data would not be acceptable for public posting on the University website, it must not be entered into a public AI Tool.

1. AI Use Disclosure Guidance

Users must ensure transparency when AI Tools meaningfully contribute to University work products. To support integrity, trust, and accountability, the following disclosure guidelines apply:

a) **No disclosure required** when AI support is minimal (e.g., grammar correction, formatting, spell-checking, readability adjustments; ~0–10% contribution)

b) **Disclosure recommended** when AI assists in shaping content or structure (e.g., drafting sections, summarizing notes, outlining ideas, generating concept language; ~10–50%)
c) **Disclosure required** when AI produces a substantial portion of the work (e.g., producing most text, generating report content, drafting communications; >50%)
d) **Supervisor notification and review required** when AI generates the majority or entirety of final content (>75%). In addition to disclosure, the employee must inform their direct supervisor prior to issuance to ensure appropriate human oversight and accountability.

2. Legal and Regulatory Compliance

Use of AI tools must comply with all applicable laws and University obligations, including but not limited to:

a) FERPA (student educational records)
b) HIPAA (protected health information, if applicable)
c) GLBA (financial information)
d) Missouri Sunshine Law (public records & retention)
e) Copyright and intellectual property law
f) Contract and software license terms
g) Anti-discrimination and bias laws (federal and state)
h) Biometric and likeness protections (where applicable)
i) Accessibility requirements (ADA Section 504/508)

AI outputs do not exempt users or the University from compliance requirements.

The University in consultation with the Office of General Counsel will review and refine applicable references as regulations and guidance evolve.

3. AI Use of Personal Voice, Image, and Likeness

The University shall not create, replicate, synthesize, or otherwise use a person's voice, image, biometric data, or personal likeness using AI technologies without:

a) Informed written consent from the individual;
b) Clear disclosure of how and where the likeness will be used;
c) Defined retention period and destruction parameters;
d) Right to revoke consent at any time without retaliation;

e) Review and approval by Technology Services and Human Resources (or designated authority).
f) Employees, students, and affiliates shall not be required to provide their likeness, voice, or biometric data for AI systems as a condition of employment, participation, or service.

4. Prohibited Conduct: Deceptive or Harmful AI Use

The use of AI Tools to impersonate, manipulate, or misrepresent real individuals is strictly prohibited. Users shall not generate, alter, or distribute AI-produced content that:

a) Creates deepfakes or synthetic likenesses of individuals without informed consent;
b) Fabricates voices, images, or video to deceive, harass, threaten, defame, or mislead others;
c) Produces sexually explicit or exploitative content involving real individuals (including students, staff, and faculty), regardless of whether the material is consensual or altered;
d) Mimics University leaders, officials, or departments to obtain information, influence actions, or commit fraud; or
e) Misrepresents official communications or creates false University materials.

Such conduct will be considered a serious violation of University policy and may result in disciplinary action up to and including termination, expulsion, or referral to law enforcement.

C. Academic and Student Usage

Academic and instructional AI use falls under the authority of Academic Affairs and faculty governance. Faculty may incorporate AI tools, including publicly available generative AI systems, into teaching and learning activities at their discretion consistent with this policy.

Unless authorized by the faculty member, in general students shall not use AI Tools to replace original thought or critical engagement with the material being studied. Students are expressly prohibited from using AI to attend and/or transcribe or record any meeting, lecture, or any other form of communication, in either audio or written format absent.

D. Governance, Risk Management, and Oversight

Technology Services oversees this policy in coordination with Risk Management, Office of General Counsel, and Academic Affairs through the **AI Advisory Group**.

The AI Advisory Group consists of representatives from Technology Services, Risk Management, General Counsel, Academic Affairs, and other relevant operational units as designated by the Chief Information Officer (CIO).

The AI Advisory Group:

a. Reviews and provides recommendations on high-impact administrative AI use;
b. Evaluates vendor security, privacy, and accessibility;
c. Coordinates updates, training, and compliance monitoring; and
d. Implement a monitoring process consistent with the NIST AI Risk Management Framework (AI 600-1).

Final authorization for high-impact AI deployments is issued by Technology Services in consultation with the AI Advisory Group. Requests for exceptions to AI system deployment, data use restrictions, or disclosure requirements under this policy must be submitted in writing to Technology Services for review, documentation, and, where appropriate, consultation with the AI Advisory Group.

E. AI Agents and Autonomous Actions

AI Tools and systems that perform autonomous or semi-autonomous actions ("AI Agents") must not be deployed without prior review and authorization from Technology Services.

1. AI Agents include systems that can:

    - Send emails or messages automatically
    - Create, modify, or delete digital records
    - Trigger workflows or approvals
    - Interact with enterprise systems or student information systems
    - Perform scheduled tasks without direct human action

2. Requirements:

    - A human must remain responsible for oversight
    - Output or actions must be reviewable and auditable
    - Agents may not make binding decisions affecting employment, student status, academic records, or finances
    - Automated interactions with University systems must follow access control and data governance requirements

3. Deployment is prohibited without:

    - Documented use case
    - Data classification review
    - Security and access controls
    - Human-approval checkpoints
    - Formal authorization from Technology Services

F. Data Privacy and Model Training

a. Prompts and outputs created within University Google Workspace for Education services (including Gemini for Education and NotebookLM) are treated as customer data under Google's Data Processing Addendum and are not used to train Google's models without explicit consent.
b. University administrators will configure Gemini Apps Activity and NotebookLM settings to prevent training on institutional content wherever technically feasible; feedback mechanisms that could share content externally will be disabled for Restricted OUs.

c. Third-party AI systems integrated via APIs or add-ons must not transfer University data for generalized model training or external analytics.
d. All data entered into AI systems is subject to records-retention, public records, and privacy policies of the University and applicable law.

G. Administrative Controls

Access to AI services will be role-based and limited to approved organizational units (OUs) or groups.

System administrators will apply data-loss-prevention (DLP) policies, sharing restrictions, and audit logging to monitor activity consistent with risk.

The University will maintain an inventory of Authorized AI System's and AI Tools, including vendor compliance statements, security certifications, accessibility conformance (VPAT), and data-handling practices.

Future AI Tools must undergo vendor risk, accessibility, and privacy review before deployment.

H. Security and Compliance Framework

The University aligns its AI governance with applicable laws and sector guidance, including: FERPA; GLBA (as applicable); HIPAA (where applicable); the CISA AI Data Security guidance; EDUCAUSE ethical AI principles; accessibility standards (WCAG 2.1 AA/Section 508); PCI-DSS, and the NIST Artificial Intelligence Risk Management Framework (AI 600-1) and University information-security policies.

This policy and its associated appendices align with the NIST AI Risk Management Framework (AI 600-1) and the Missouri Department of Elementary and Secondary Education's (DESE) *Artificial Intelligence Guidance for Local Education Agencies* (2025-26).

Together, these regulations and frameworks provide foundational principles for transparency, accountability, and ethical AI use in education.

I. AI Training and Awareness

The University will provide and periodically update AI literacy and data privacy training for employees and authorized users. Completion of AI training is required before accessing institutional AI tools such as Gemini for Education or NotebookLM. Training will address ethical use, data classification, bias awareness, and compliance with applicable University, state, and federal regulations. Supplemental training may be assigned based on role or system access level.

Training may be delivered through the University's approved online learning platform (currently Vector Solutions) or equivalent system designated.

J. Public Records, Intellectual Property, and Records Management

AI prompts and outputs related to University business may constitute public records under the Missouri Sunshine Law (RSMo Chapter 610) and are subject to disclosure unless an exemption applies.

Ownership of AI-assisted works created in the course of employment follows University IP policy and applicable contracts; third-party content and licensing obligations must be respected.

AI-generated content stored in University systems is subject to records retention, litigation hold, and e-discovery requirements consistent with University policy.

K. Third-Party API Use

Applications accessing University data via Application Programming Interfaces (APIs) must comply with the University vendor-risk process, DPA requirements, and must not use University data to train generalized models.

Only University approved APIs or third-party integrations may be enabled; high-risk scopes require explicit approval and least-privilege access.

L. Incident Reporting and Enforcement

Suspected security incidents, privacy breaches, or policy violations involving AI Tools must be reported immediately to the Chief Information Security Officer.

Misuse of AI Tools may result in loss of access and disciplinary action under applicable HR or student-conduct policies.

M. Review and Revision

This policy will be reviewed as needed by the AI Advisory Committee or equivalent body. Updates will account for emerging regulations, vendor changes, and audit findings.

Policy History

Date of Review/Revision	Summary of Change

APPENDIX A

Implementation and Vendor Evaluation Framework

A.1 Google Workspace (Gemini and NotebookLM) Implementation Summary

Control Area	Gemini / NotebookLM Setting	University Implementation
Training on prompts	Gemini Apps Activity; Feedback collection	Disabled by default for administrative and instructional OUs.
Data classification	Workspace DLP rules; Shared-drive controls	Restricted data blocked; confidential data requires encryption/approval.
Service availability	Enable/disable per OU or group	Faculty/staff pilot; student access subject to separate review.
Data export & retention	Workspace retention; Vault	Follow institutional retention schedule; logs retained ≥30 days.
Third-party access	Workspace Marketplace apps	External integrations require vendor-risk and data-protection review.
FERPA compliance	Google for Education Core Service	Affirmed under Google DPA; no training on customer data.
Audit logging	Admin console; BigQuery exports	Quarterly monitoring for unusual usage patterns.

A.2 Future Vendor Evaluation Criteria

Evaluation Domain	Key Questions / Criteria	Acceptable Standard or Documentation
Data Protection & Model Training	Does vendor prohibit training on customer data?	DPA clause: no model training on customer data; opt-out by default.
Privacy Compliance	FERPA/GLBA/HIPAA/GDPR compliance?	SOC 2 Type II, ISO 27001, DPA, privacy notices.
Data Residency & Ownership	Where is data stored/processed? Who owns outputs?	Data-location docs; customer data ownership retained.
Security Controls	Encryption, SSO/SAML, logging?	AES-256 at rest, TLS 1.2+ in transit; SSO; audit trails.
Admin Controls	Role/OU scoping, DLP/retention available?	Granular admin console/API; DLP policies; retention settings.

Transparency & Explainability	Documented limitations/biases/sources?	Model cards; transparency reports.
Accessibility & Inclusion	WCAG 2.1 AA / Section 508 conformance?	VPAT provided and reviewed.
Academic Freedom & IP	Does platform preserve user/IP rights?	TOS retains user/institution ownership of content.
Cost & Licensing	Transparent pricing; contract terms?	Price sheet; renewal, exit, SLA terms specified.
Integration & Interop	Secure interop with Google Workspace/LMS/ERP?	API docs; sandbox testing; security review results.
Support & Deactivation	Deprovisioning; data deletion at end of term?	Contractual data-deletion and off-boarding procedures.

A.3 Approval Process for New AI Services

- Proposal Submission: Department submits purpose, scope, user roles, and expected benefits.
- Preliminary Review: Technology Services & Risk Management conduct vendor-risk and data-protection assessment using A.2.
- Committee Recommendation: AI Advisory Group evaluates alignment with mission, ethics, and resources.
- Executive Approval: Final authorization by Technology Services or designee.
- Pilot Implementation: Limited rollout with defined success metrics and security controls.
- Annual Review: Vendor re-evaluated for compliance, cost, accessibility, and emerging risks.

A.4 Cross-Vendor Governance Principles

Promote environmental sustainability: Vendors should disclose known energy consumption and carbon impacts associated with large-scale model training or operation, aligning with institutional sustainability goals.

- Protect institutional data consistent with CISA AI Data Security and University DLP standards.
- Provide administrative transparency into configuration and access logs.
- Allow opt-out of data use for model training without loss of core functionality.
- Support FERPA and accessibility compliance; provide VPAT and privacy documentation.
- Include clear end-of-service data removal and return provisions.

APPENDIX B

AI Use Disclosure Guidance

Disclosure protocols should be tailored to the specific context in which the work is produced and disseminated. Always verify institutional, departmental, journal, or platform-specific policies for disclosure of AI use before publishing or submitting content. Disclosures must be proportionate and specific, reflecting the actual role of AI in the work.

Please consider the following practices to help ensure transparency, accountability, and compliance with ethical standards and legal requirements.

AI use does not always need to be publicly disclosed when the final version has been reviewed and approved by a human prior to publication.

AI use should be disclosed in writing when any of the following apply:

Legal, Policy, or Platform Requirements

- Disclosure is required by law, vendor policy, or platform rules (e.g., YouTube, Instagram).
- Action: Check and comply with each platform's specific attribution rules.

Lack of Human Oversight

- The content cannot be reviewed by a knowledgeable human professional communicator or subject-matter expert before publication (e.g., chatbot replies, dynamically generated output, automated outputs).

AI-Created or AI-Modified Media

- Images or videos were generated using AI tools.
- Existing visuals were altered by AI in a way that changes facts, meaning, or context.

Substantive AI Contribution

- AI contributed in a meaningful or creative way—for instance:
- Generating or organizing core ideas or hypotheses
- Drafting or summarizing major sections of text
- Conducting or structuring an analysis
- In these cases, AI acted beyond a supportive tool and should be acknowledged.

Unless required in specific contexts, disclosure may not be needed when AI is used only for minor or stylistic assistance, such as:

- Grammar, spelling, or formatting corrections

- Text cleanup or readability improvements
- Routine data visualization or layout adjustments

When disclosure is required, it should be clear, brief, and placed directly with the content.

When disclosure is warranted, the method and placement should be appropriate to the audience and context:

- Public-facing materials (e.g., websites, publications, patient communications) include a conspicuous and visible footnote, acknowledgment, or statement.
- Internal communications: apply discretion, though transparency is encouraged.

When applicable, cite AI-generated content according to the relevant formal style guide (APA, MLA, Chicago, or AP Style).

Suggested Disclosure Language

At Missouri Western, we believe in the power of technology and are committed to using artificial intelligence (AI) responsibly. Please note that [name of AI tool] was used to assist in generating [brief description of content]. While AI contributed to this content, it has been reviewed and approved by [name or role of the responsible individual or office].

When AI is used to create multimedia content (e.g., digital portraits or synthetic audio), a clear disclaimer should accompany the content. This disclaimer should identify the tool used and describe its role in the creative process.

Background and References

a. National Institute of Standards and Technology (NIST). (2025). AI 600-1: Generative Artificial Intelligence Risk Management Framework (GAIRMF). Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
b. Missouri Department of Elementary and Secondary Education (DESE). (2025). Artificial Intelligence Guidance for Local Education Agencies (LEAs) 2025–26. Available at: https://dese.mo.gov/
c. Taxonomy of AI Risks. (2024). Overview document outlining risk types and governance recommendations for educational institutions.
d. Lindenwood University. (2024). AI Use in Employment Policy. Example of higher education policy application referenced for benchmarking.
e. Emory University. When and How to Disclose AI Use.