Missouri Western State University

Policy Name: Artificial Intelligence (AI) Use and Governance Policy	**Date Effective**: July 1, 2026
Policy Category: Information Security; Data Governance; Academic Affairs	**Date Last Revised**:
Approval Authority: Vice President for Finance and Administration	**Date Last Reviewed:**
Responsible Office or Official: Technology Services	**Review Cycle**: 3 years

I. Purpose/Policy Statement

Missouri Western State University (MWSU) recognizes the transformative potential of Artificial Intelligence (AI) technologies to improve efficiency, insight, and decision-making across university operations.

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.

The policy aligns with applicable regulations and frameworks, including FERPA, HIPAA, GLBA, PCI-DSS, and the NIST Artificial Intelligence Risk Management Framework (AI 600-1).

II. Scope and Applicability

This policy applies to all University employees, student workers, 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).

Personal or consumer accounts are outside the scope of institutional authorization for handling institutional data.
This policy governs administrative and operational use; academic instruction and research uses are covered separately under Academic Affairs policies.

III. Definitions

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, managed, and secure AI platform integrated into MWSU systems.

Public AI Tool: Any publicly available AI service not managed by MWSU.

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).

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

1. Data Classifications:
   a) Confidential: Highly restricted (e.g., SSNs, credit-card numbers). Never permitted in any AI tool.
   b) Sensitive: Protected data (FERPA, HIPAA, etc.); prohibited in public AI tools.
   c) Internal: Operational data not for public release; limited use with caution.
   d) Public: Data already publicly available through official University channels.
   e) 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.

IV. Acceptable and Prohibited Use - Handling Requirements

a) Use of AI tools must comply with the University's Data Classification Policy. Confidential and Restricted data are prohibited in public AI tools and may only be used in University-approved systems with appropriate safeguards.
b) Confidential Data must not be entered into any AI system unless formally authorized by the Chief Information Security Officer (CISO) or designee and subject to a Data Protection Addendum (DPA) and security controls.
c) 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.
d) 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.
e) Personal experimentation with public AI systems must not involve University data or credentials.

V. 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 below.
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.

2. **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).

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.

3. **C. Prohibited Conduct: Deceptive or Harmful AI Use**

The use of AI technologies 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
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.

VI. Academic and Student Use

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. However, institutional data classification requirements and applicable privacy laws remain in effect. Confidential or regulated University data may not be entered into public AI systems.

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.

Legal Counsel will review and refine applicable references as regulations and guidance evolve.

VII. Governance and Oversight

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

1. **AI Advisory Group**

The AI Advisory Group consists of representatives from Technology Services, Risk Management, Legal Counsel, Academic Affairs, and other relevant operational units as designated by the 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.

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.

VIII. AI Agents and Autonomous Actions

AI 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:
   a) Send emails or messages automatically
   b) Create, modify, or delete digital records
   c) Trigger workflows or approvals
   d) Interact with enterprise systems or student information systems
   e) Perform scheduled tasks without direct human action

2. Requirements:
    a) A human must remain responsible for oversight
    b) Output or actions must be reviewable and auditable
    c) Agents may not make binding decisions affecting employment, student status, academic records, or finances
    d) Automated interactions with University systems must follow access control and data governance requirements

3. Deployment is prohibited without:
    a) Documented use case
    b) Data classification review
    c) Security and access controls
    d) Human-approval checkpoints
    e) Formal authorization from Technology Services

IX. 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.

X. Administrative Controls

a) Access to AI services will be role-based and limited to approved organizational units (OUs) or groups.
b) System administrators will apply data-loss-prevention (DLP) policies, sharing restrictions, and audit logging to monitor activity consistent with risk.
c) The University will maintain an inventory of approved AI services, including vendor compliance statements, security certifications, accessibility conformance (VPAT), and data-handling practices.
d) Future AI services must undergo vendor risk, accessibility, and privacy review before deployment.

XI. 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); and University information-security policies.

XII. 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.

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

XIII. Public Records, Intellectual Property, and Records Management

a) Public Records: 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.
b) Intellectual Property: 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.
c) Records Retention and E-Discovery: AI-generated content stored in University systems is subject to records retention, litigation hold, and e-discovery requirements consistent with University policy.

XIV. Third-Party & API Use

a) Applications accessing University data via APIs must comply with the University vendor-risk process, DPA requirements, and must not use University data to train generalized models.
b) Only approved Marketplace or third-party integrations may be enabled; high-risk scopes require explicit approval and least-privilege access.

XV. Incident Reporting and Enforcement

a) Suspected security incidents, privacy breaches, or policy violations involving AI services must be reported immediately to the Technology Services and Risk Management.
b) Misuse of AI tools may result in loss of access and disciplinary action under applicable HR or student-conduct policies.

XVI. Review and Revision

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

This policy will be reviewed at least annually by the AI Governance Committee or equivalent body under the Division of Administration and Technology. Updates will account for emerging regulations, vendor changes, and audit findings.

XVII. 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.

A.5 Policy Revision History

Version	Date	Description of Changes	Approved By
1.0		Initial policy adoption and framework establishment	

AI Risk Monitoring and Measurement

The AI Advisory Group will implement a monitoring process consistent with the NIST AI Risk Management Framework (AI 600-1). This includes identifying, mapping, and periodically evaluating AI-related risks across system lifecycles. Metrics may include model accuracy, bias detection, information integrity, and data-protection compliance. Findings from these assessments will inform continuous policy improvement and risk mitigation strategies.

XVIII. Appendix B – AI Risk Domains (per NIST AI 600-1)

The following domains reflect common risk areas identified by NIST and complementary guidance from the Taxonomy of AI Risks framework. These domains are considered during AI system evaluation, procurement, and deployment:

a) Accuracy and Reliability – Monitoring of AI system outputs to prevent confabulation or 'hallucination.'
b) Bias and Fairness – Evaluation for potential algorithmic or dataset bias impacting outcomes.
c) Data Privacy and Protection – Ensuring proper data minimization, anonymization, and encryption controls.
d) Information Integrity – Preventing misinformation or manipulation through AI-generated content.
e) Human–AI Interaction and Oversight – Guarding against automation bias and over-reliance.
f) Accountability and Transparency – Clear documentation of decision-making processes and provenance tracking.
g) Intellectual Property and Legal Compliance – Preventing unauthorized reuse or copyright infringement.
h) Security and Cyber Risk – Managing vulnerabilities in API integrations or third-party model access.
i) Environmental Sustainability – Evaluating energy use, carbon footprint, and lifecycle impacts of AI systems.
j) Accessibility and Inclusion – Ensuring all AI tools meet accessibility standards (WCAG 2.1 AA / Section 508).

XIX. Appendix C – 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.