Millersville University **Governance & Policies**

Effective: December 1 2025

Information Technology Policy
Acceptable Use of Artificial Intelligence

Approved: December 1 2025
President's Cabinet

Artificial Intelligence (AI) technologies are increasingly integrated into teaching, research, and administrative activities. While AI provides powerful tools to enhance learning, decision-making, and innovation, its use must remain consistent with the University's mission, values, and policies. This policy establishes expectations for the ethical, transparent, and responsible use of AI by all members of the University community.

1. Purpose and Scope

This policy outlines the ethical and responsible use of AI technologies in academic and administrative functions at Millersville University.

AI includes, but is not limited to, generative AI, machine learning applications, automated decision-making systems, and agentic AI.

Sections 2–5 establish baseline expectations for responsible AI use across the University. Section 6 provides additional requirements for agentic (autonomous) systems that operate with higher levels of independence and institutional risk.

2. Ethical Use

- AI should augment, not replace, human decision-making and learning.
- Users must validate AI-generated content for accuracy, fairness, and ethical implications.
- AI must not be used for deepfakes, misinformation, or academic dishonesty.
- Individuals remain accountable for all outputs, decisions, and actions informed by AI, and must be prepared to disclose and explain their use of AI tools when requested.
- AI must never be the sole basis for decisions that significantly affect individuals; meaningful human oversight is always required.

3. Academic Integrity

- AI-generated content used in coursework or research must be cited following the Student and Faculty Academic Honesty Policies.
- Use of AI tools in assignments or assessments is permitted only in accordance with the University's Student Academic Honesty Policy.
- Students must follow the expectations outlined in that policy and obtain explicit instructor approval before incorporating AI-generated content into their academic work.

4. Data Privacy and Compliance

- Users must not input personally identifiable information (PII), confidential University data, or proprietary research into public AI systems.
- AI systems utilizing University data must comply with University data governance standards and all applicable federal, state, and local laws (e.g., FERPA, HIPAA).
- Procurement and adoption of third-party AI applications must include University IT and procurement review to ensure compliance with data protection, security, and accessibility standards.

5. Research and Innovation

- Researchers using AI must adhere to ethical research standards, ensuring transparency in AI-driven methodologies.
- AI applications must undergo risk assessments for bias, security vulnerabilities, and compliance with University policies.
- Research projects utilizing AI that involve human subjects must obtain approval from the University's Institutional Review Board (IRB) to ensure compliance with federal regulations, ethical standards, and participant protections.

6. Agentic Artificial Intelligence (AI Agents)

As AI capabilities evolve toward greater autonomy, the following section establishes additional guidance for agentic AI systems that can act on behalf of individuals or the institution. These provisions reflect the higher level of oversight, accountability, and risk management required for such technologies.

Definition
Agentic AI refers to artificial intelligence systems that can independently perform multi-step tasks or make autonomous decisions on behalf of users or the institution.

Unlike generative chatbots that only respond to prompts, agentic AI may access institutional data or systems and act with varying levels of independence.

6.1 Institutional Oversight and Shared Accountability

- Every deployment of agentic AI must have a University sponsor (academic or administrative unit) and a designated human supervisor responsible for oversight.
- Oversight will follow a risk-based review process:
    - **Low-risk** (e.g., instructional support, scheduling assistants): self-disclosure to IT, tracked via the AI Inventory.
    - **Moderate-risk** (e.g., advising or communications bots accessing limited data): departmental review and documentation.
    - **High-risk** (e.g., systems influencing grades, financial aid, admissions, or employment): formal review by IT Security, Data Governance, and Risk Management.
- Units are expected to maintain local accountability for the safe and ethical operation of their approved agentic AI systems.

6.2 Transparency and User Disclosure

- Users interacting with agentic AI must be informed they are engaging with a digital system, not a human.
- Agentic AI must maintain basic activity logs to ensure accountability and allow for investigation if needed.
- Significant institutional decisions (academic, financial, or employment-related) must always include a human verification step before action.

6.3 Data Governance and Security

- Agentic AI must operate within approved and secure University environments.
- Agents should be granted the minimum level of access necessary to perform their tasks.
- Agents accessing institutional data must be registered in the AI Inventory and comply with existing University data protection and accessibility standards.
- Regular review cycles may be coordinated through existing audit or IT security processes, not as separate procedures.

6.4 Academic and Research Use

- Faculty and researchers employing agentic AI must disclose its use in syllabi, project documentation, or publications as appropriate.
- Student use of agentic AI must follow the University's Academic Honesty Policy and instructor guidelines.
- Research involving human subjects and agentic AI must adhere to existing IRB review requirements.

6.5 Ethical and Operational Safeguards

- Agentic AI must support the University's EPPIIC values: Exploration, Professionalism, Public Mission, Inclusion, Integrity, and Compassion.

- All systems must include a human override mechanism to immediately suspend or stop an AI agent's actions if unintended behavior occurs.
- Agentic AI may not impersonate University employees, misrepresent authority, or collect personal information without consent.
- Where possible, existing University platforms (e.g., LMS, SharePoint, CRM) should be used to host or integrate agentic AI functions rather than developing standalone, unsupervised systems.

6.6 Continuous Improvement and Reporting

- Departments piloting agentic AI should document lessons learned and share them with the University AI Committee to inform institutional policy and best practices.
- Annual updates to the AI Committee may focus on aggregate trends and risks, not individual project audits.
- As the AI landscape evolves, the University will periodically review and scale oversight procedures to balance innovation, risk, and staffing capacity.

7. Related Policies

- PASSHE IT Acceptable Use Policy
- Student Academic Dishonesty Policy
- Faculty Policy Academic Dishonesty and Plagiarism
- Electronic Data Classification and Handling
- University Institutional Review Board