



Artificial Intelligence (AI) Acceptable Use Policy

TEC 21.0

Information Technology

Policy Type: Administrative

Applies to: Faculty, staff, students, volunteers, contractors

POLICY DATES

This policy supersedes and replaces all other policies prior to this revised date.

Issued: July 2026

Revised:

Edited by: Tina Stuchell, Patrick Heddleston

Table of Contents

Overview

Definitions

Policy Details

Purpose & Scope

Institutional Guiding Principles

Alignment with NIST AI RMF

- Govern
- Map
- Measure
- Manage

Acceptable AI Use

Prohibited Uses

Overview

The University of Mount Union is dedicated to advancing knowledge and learning and embraces innovative technology such as Generative Artificial Intelligence (AI) tools as defined below. We encourage faculty, staff and students to explore and experiment with these tools. Generative AI tools have the capacity to expedite existing processes and make new ones and have the potential to improve student learning and advance research. While the University of Mount Union supports the responsible use of AI, these tools have limitations and present new risks that must be considered when using AI technology.

Two key risk attributes of these Generative AI tools are that an input can potentially become public, and the risk that an output may be biased, misleading, or inaccurate. These risks could include information security, data privacy, copyright, academic integrity, and bias. Examples of such risks include:

- Generative AI should never be given access to personal information, as its technology may not respect the privacy rights of individuals and could create compliance issues with data protection laws.
- Generative AI should not be given access to confidential information or trade secrets of the University, including intellectual property (IP) rights to that information, as the University could lose such IP rights and/or the information may be disclosed to unauthorized third parties through their independent use of the same Generative AI.
- Generative AI may violate IP rights of others and might not themselves be protected by appropriate IP laws.
- Generative AI outputs may be factually inaccurate, and the University could be exposed to liability if it relies on those outputs without proper review by the appropriate, qualified individuals.
- Generative AI may produce decisions that are biased, discriminatory, or otherwise inconsistent with University policies or that violate applicable laws or regulations.

Definitions

Term	Definition
Artificial Intelligence (AI)	Computer systems or technologies capable of performing tasks that typically require human intelligence, including learning, reasoning, pattern recognition, content generation, and decision support.

Artificial Intelligence (AI) Acceptable Use

TEC 21.0

Information Technology

Term	Definition
Generative AI	Any machine-based tool capable and designed to consider user questions or the creation of new content such as text, images, audio, video, code, or data based on training data and user prompts, including, for example purposes, ChatGPT, Claude, Gemini.
AI Generated Content	Any output created partially or wholly by an AI system.
Confidential Information	Any business or technical information or result of research belonging to the University of Mount Union, a University Community member, collaborators, or other third parties, which is publicly not known or that has been provided or received under an obligation to maintain the information as confidential.
Personally Identifiable Information (PII)	Data, whether alone or in combination with other available information, that can be used to identify, relate to, or describe an individual, including but not limited to, name, identification number, email address, or demographic information.
Sensitive Data	Data that, if compromised, could cause harm to individuals or the institution, including PII, education records, financial data, health information, biometric data, and other regulated or confidential information.
University Approved AI Tools	AI systems that have been reviewed and approved by the University for use with institutional or regulated data.
FERPA	Family Educational Rights and Privacy Act. Federal law protects the privacy of student education records.
HIPAA	Health Insurance Portability and Accountability Act. Federal law is designed to protect sensitive patient health information from disclosure without consent. Mandates privacy and security safeguards for protected health information (PHI)
GLBA	Gramm-Leach Bliley Act. US Federal law requires protection of sensitive customer data. Mandates security safeguards.
GDPR	General Data Protection Regulation. A comprehensive European Union (EU) law governing data protection and privacy, applying to any entity processing personal data of EU residents. Grants individuals control over their data and mandates strict compliance for organizations.
NIST	The National Institute of Standards and Technology (NIST) is a U.S. government agency within the Department of Commerce. This agency develops cybersecurity frameworks, technical standards and promotes industrial innovation and competitiveness.

Policy Details

This policy is meant to provide an overarching set of institutional guidelines and works in tandem with the Faculty and Instructional Staff Use of AI [POLICY](#), as well as a student use of AI, which is located within the student handbook [POLICY](#).

Purpose & Scope:

The University of Mount Union is committed to the responsible, ethical, and secure use of Generative AI technologies in support of its educational mission, institutional operations, and community values. The University expects that all its community members, including staff, faculty, students, contractors, researchers and affiliates (collectively, the “University Community”) will follow these guidelines when using AI tools for teaching and learning, research and work-related functions.

Artificial Intelligence (AI) Acceptable Use

TEC 21.0

Information Technology

This Generative AI policy (the “Policy”) governs the use of Generative AI technologies by the University Community in the performance of their functions for or on behalf of the University. This Policy establishes expectations and responsibilities for the use of AI systems to:

- Promote innovation, learning, and operational effectiveness.
- Protect institutional, personal, and regulated data.
- Align use of AI with applicable laws, regulations, and University policies.
- Manage risks associated with AI in accordance with the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF)

This Policy applies to all members of the University Community, and governs the use of AI technologies in academic, administrative, research, and operational contexts, including:

- AI tools are accessed using University owned or personal devices when used for University related activities.
- AI systems licensed, supported, or approved by the University.
- External or third-party AI tools used in connection with University work.
- Academic uses of AI in teaching, learning, and assessment are additionally governed by the Faculty and Instructional Use of Artificial Intelligence Policy.

Acquisition of AI Products

The Office of Information Technology (IT) of the University must be contacted before the purchase of AI products (including the use of free applications) or products that contain functions that rely on AI to operate. IT must evaluate and approve the use of such products on the University’s network in advance of, and as a condition to any such use.

IT may publish a list of specific AI applications that have been vetted by the Office and deemed fully or partially acceptable under this Policy, which list will be subject to change by IT from time to time and each University Community Member will be responsible for ensuring that any AI applications used thereby are identified on the then-current list. A list of supported software can be found here: https://experience.elluciancloud.com/umu/page/approved_software

Institutional AI Guiding Principles:

Artificial Intelligence is the science of making machines that can simulate human intelligence. The University created AI guiding principles in 2024, as stated below, and under the IT Resources tab at [POLICY](#):

The purpose of these guiding principles, as an institution of learning, is to outline the University’s commitment to responsible, ethical, and beneficial AI development and deployment, ensuring that its AI systems align with the University’s mission and values and contribute positively to society.

We strive to:

1. **Make ethical choices.** We will ensure integrity is the highest priority. We will address bias, fairness, privacy, transparency, and accountability in all AI-related decisions.
2. **Leverage AI to Empower Institutional Success.** We will embrace AI’s potential to enhance our capabilities, stimulate innovation, and drive operational efficiency.
3. **Keep “Humans in the Loop.”** We will maintain the perspective that AI cannot substitute for human judgment. AI should never replace human judgment.
4. **Respond to Continuous Change.** We will balance careful consideration, agility, and urgency to respond to continuous change.

Artificial Intelligence (AI) Acceptable Use

TEC 21.0

Information Technology

5. **Safeguard Confidential Information.** We will protect confidential information through security measures. We will follow data privacy regulations and strive to protect UMU faculty, staff and student data.

These guiding principles have been developed in alignment with the University's values and The National Institute of Standards and Technology (NIST) Trustworthy AI principles, and members of the University Community must follow the institution's AI guiding principles, and all AI tools must align with these principles.

Acceptable AI Use

NIST AI Risk Management Framework

The University aligns its AI use with the [National Institute of Standards and Technology](#) (NIST) and AI RMF [AI Risk Management Framework | NIST](#) Core Functions: **Govern, Map, Measure, and Manage**, to support trustworthy and responsible AI adoption.

GOVERN (Oversight and Accountability)

- AI use must comply with applicable laws, regulations, contractual obligations, and University policies, including FERPA, HIPAA, GLBA, GDPR as applicable as well as general information security standards.
- The University establishes governance structures to oversee AI use, including the approval of institutionally supported AI tools.
- Users remain fully accountable for decisions, actions, and outcomes informed or assisted by AI systems.
- AI tools shall not be used to make final determinations involving academic evaluation, employment actions, disciplinary decisions, or other high impact outcomes without human review and approval.

MAP (Context and Risk Awareness)

Before using AI tools for University purposes, users must consider:

- The purpose and context of the AI use.
- The sensitivity and classification of data involved.
- Potential impacts on individuals, academic integrity, and institutional operations
- AI systems vary in capability, reliability, and risk profile. Users must assess whether AI use is appropriate for the specific task and context.

MEASURE (Evaluation, Accuracy, and Bias)

- AI -Generated content may be inaccurate, incomplete, biased, or misleading; therefore, University of Mount Union community members must check the accuracy of information generated by Generative AI tools prior to relying on such information.
- Users must verify AI outputs using credible and independent sources before relying on them for academic, professional, or operational purposes.
- AI output must be reviewed for bias, fairness, appropriateness, and accuracy; therefore, University of Mount Union community members must consider whether the data input into, and the output of, Generative AI tools produce decisions that may result in a disparate impact to individuals based on their protected classifications under applicable law.

MANAGE (Risk Mitigation and Continuous Improvement)

- Sensitive, regulated, or non-public University data may only be used with **University-Approved AI tools**.

Artificial Intelligence (AI) Acceptable Use

TEC 21.0

Information Technology

- Users must not input sensitive data, PII, education records, health information, proprietary information, or copyrighted material into unapproved AI systems.
- Suspected AI misuse, data exposure, or unintended consequences must be reported to a supervisor, Information Technology, or another appropriate University office.
- Violations of this Policy may result in disciplinary action consistent with University policies and procedures.

Acceptable Use Responsibilities:

All users must:

- Use AI as a tool to support, not replace critical thinking and human judgment.
- Comply with all University policies, standards, and guidelines.
- Respect intellectual property rights and academic integrity.
- Use only approved AI tools when working with sensitive or regulated data. (See MANAGE section)
- Disclose when AI tools are used to generate or substantially assist professional or academic work, in accordance with applicable academic or departmental guidelines.
- University Community members who leverage Generative AI to produce written materials or other work product must disclose that those materials and that work product are based on or derived from the use of Generative AI.
- Always verify information using credible sources, as AI outputs can be inaccurate, biased, misleading or fabricated.
- Opt-out of the use of data within Generative AI systems to train future iterations of the Generative AI system. When made available, University of Mount Union community members are expected to opt out of training,

Prohibited Uses:

University Community members must **NOT**:

- **Input confidential information, PII, restricted or otherwise sensitive information.** University Community members must refrain from inputting confidential information or PII except when expressly permitted to do so by a validated contract or release and with appropriate security controls, in each case approved by the IT Department of the University.
- **Input or use information that violates contract terms and conditions.** University Community members must be aware of the terms and conditions under which they are using AI tools, with the goal of complying with such terms and conditions.
- **Input or use information that violates IP rights.** University Community members must respect the IP rights of University Community members, the University, and third parties, with the goal of protecting those IP rights. This includes ensuring that, under applicable vendor licenses governing any digital resources provided by the University, that use of their content with AI tools is permitted, and ensuring that the inputs and outputs of the AI tools are properly protected under applicable patent and copyright laws, data protection regulations, and identity theft regulations. In addition, University Community members must not hold out any output generated by Generative AI as their own and, in quoting or paraphrasing or borrowing ideas from the output of Generative AI, confirm that the output is accurate and that the use does not constitute plagiarism of another party's existing work and does not otherwise violate another party's IP rights.
- **Exclusively use AI-Generated content.** University Community members must not rely exclusively on and must check the accuracy of AI-Generated Content, including, but not limited to, confirmation of accuracy using additional resources.
- **Use AI to violate federal, state, or local laws.**
- **Use AI to engage in discrimination, harassment, stalking, or exploitation.** University Community members must evaluate and be aware of whether the Generative AI data inputs and outputs produce decisions or results

Artificial Intelligence (AI) Acceptable Use

TEC 21.0

Information Technology

which may result in a disparate impact on or otherwise discriminate against individuals based on their protected classifications (ex: race, ethnicity, nationality, age, sexual orientation or disability) under applicable laws.

- **Use AI to generate malware, bypass security controls, or facilitate cybercrime.** University Community members are prohibited from using Generative AI tools to generate malicious content, such as malware, viruses, worms and trojan horses, that may have the ability to circumvent access control measures in place by the University or any third-party individual or entity to prevent unauthorized access to their respective networks.
- **Use AI to create fake credentials, fraudulent research, or deceptive content.**
- **Use AI to intentionally violate University policies guidelines, or contractual agreements.**
- **Use AI-enabled web browsers when you have access to institutional customer or employee data.**

Artificial Intelligence (AI) Acceptable Use TEC 21.0 Information Technology

Responsibilities

Position or Office	Responsibilities
Information Technology	AI tool review and approval, security controls, incident response
Digital Learning	Academic AI guidance, instructional support, faculty consultation
Academic Affairs	Oversight of academic AI use and integrity
All Users	Responsible, ethical, and compliant AI use

Resources

- Faculty and Instructional Use of Artificial Intelligence
- Information Security Policy
- Technology Resources Acceptable Use Policy

Contacts

Subject	Office	Telephone	E-mail/URL
	Information of Technology	330-823-2854	IT@mountunion.edu
	Digital Learning & Design	330-823-4895	craigst@mountunion.edu