XAVIER UNIVERSITY

ACCEPTABLE USE OF ARTIFICIAL INTELLIGENCE

Effective: April 2026
Last Updated: November 2025
Last Review: January 2026
Responsible University Office: Information Technologies
Responsible Executive: Chief Information Officer
Scope: Students, full-time and adjunct faculty, staff, retirees, non-employee associates, and guests

A. REASON FOR POLICY

Purpose
This policy establishes the acceptable use of artificial intelligence (AI) tools at Xavier University to promote responsible, ethical, and secure use of AI technologies. It ensures compliance with privacy, security, academic integrity, and legal obligations while supporting innovation and academic excellence.

Scope
This policy applies to all students, faculty, staff, and third parties who access Xavier University's resources and utilize AI systems, chatbots, or related technologies in any form. It covers University-owned AI systems, third-party AI tools, and AI services accessed through University networks or accounts.

B. POLICY

Acceptable Use

1. **General Use**:
    - AI tools may be used for academic, research, administrative, or other University-sanctioned purposes.
    - Users must ensure that AI tools are implemented in ways that do not violate laws, University policies, or ethical standards.
    - AI-generated content should be reviewed for accuracy and bias before use (fact-check, review sources).

- AI tools that handle data must comply with University privacy policies, FERPA, HIPAA (where applicable), and other relevant regulations.

2. **Prohibited Data Input**:

Users must not input the following types of data into AI tools, unless the tool has been explicitly reviewed and approved by Information Technologies for such use (enterprise account):

- Personally Identifiable Information (PII), including Social Security numbers, passport numbers, and driver's license numbers.
- Student records, grades, and academic history protected under FERPA.
- Medical or health information covered by HIPAA.
- Financial data such as bank account numbers, credit card information, or payroll details.
- Credentials such as usernames, passwords, or authentication tokens.
- Proprietary business data
- Any other sensitive or classified University information.

3. **Academic Integrity & Plagiarism**:
   - Students should refer to Student Responsibilities of Upholding Academic Integrity, in the Student Handbook.
   - Faculty should refer to the Misconduct in Scholarship/Research Policy
   - Faculty members are strongly encouraged to include clear expectations in their syllabi for student use of AI in all coursework, research, and other course requirements.

4. **Ethical Considerations**:
   - AI must be used in a transparent, fair, and accountable manner.
   - AI systems must not be used in ways that engage in bias, harassment, discrimination, or violation of individual rights.
   - Users must be made aware that they are interacting with an AI system rather than a human, where applicable.

5. **Use of AI Meeting Virtual Assistants**:
   - AI meeting virtual assistants must obtain explicit authorization from all participants before joining and/or recording any meeting.
   - These bots must not be configured to automatically join all calendar meetings by default.
   - Users of these should be aware of bot integrations and review their calendar permissions to prevent unauthorized access.
   - Any AI meeting virtual assistant that requires participants to create an account prior to accessing meeting summaries must disclose this requirement in advance.
   - The use of AI meeting virtual assistants must comply with University privacy policies and applicable regulations.

6. **Prohibited Use**:

Users must not use AI tools for:

- Fraudulent, malicious, or deceptive activities.
- Generating or disseminating false, misleading, or manipulated information (e.g., deepfakes), unless for guided learning purposes.
- Unauthorized access to data or systems.
- Any action that violates a University policy.

C. DEFINITIONS

- **AI Tools**: Software applications and systems that use machine learning, natural language processing, and other AI capabilities to automate tasks, generate content, analyze data, or interact with users. Examples include ChatGPT, Microsoft Copilot, and other generative AI tools.
- **AI Chatbots**: AI-powered systems that engage in dialogue with users to provide information, guidance, or perform tasks autonomously.
- **AI Meeting Virtual Assistants:** AI-driven tools that join meetings to record discussions and generate summaries, often integrating with user calendars.

D. PROCEDURES

Reporting and Enforcement:

- Compliance with this policy may be supported through the use of technologies such as AI content detection and Data Loss Prevention (DLP) systems, where appropriate.
- Repeated and intentional violations may result in actions as outlined in the University's code of conduct, employment agreements, and other relevant policies.
- Users who inadvertently input sensitive data into unprotected AI tools must immediately report the incident to the Information Security team via ServiceDesk@xavier.edu

Responsibility

- Users are responsible for ensuring their AI usage complies with this policy and any other University policy.
- Faculty members are strongly encouraged to include clear expectations in their syllabi for student use of AI in all coursework, research, and other course requirements.
- The Information Security team is responsible for reviewing, approving, and monitoring the use of AI technologies and conducting security assessments.

E. EXHIBITS (N/A)

F. HISTORY

Drafted and reviewed: October 2025
Reviewed and approved by attorneys: October 2025
Reviewed and approved by the President's Cabinet: January 2026
Revised by Information Technologies Policies and Procedures Task Force and Information Technologies Leadership Team: January 2026
Updated and reviewed:

G. REVIEW SCHEDULE

This policy will be reviewed semi-annually and updated as necessary to accommodate emerging technologies, regulatory changes, and University needs.