4.1 Acceptable Use of AI Guidelines

Effective Date: October 22, 2024
Revised Date: August 11, 2025

---

1. Purpose

This document establishes guidelines for the fair, responsible, and ethical use of Artificial Intelligence (AI) by Arkansas State University (A-State) faculty, staff, and students from an IT security perspective. The goal is to ensure that AI is used in ways that align with A-State's academic integrity standards, protect the privacy and security of sensitive data, and support the university's commitment to innovation. These guidelines supplement the ethical use of AI document previously distributed to faculty.

---

2. Scope

These guidelines apply to all A-State employees, students, contractors, and affiliated parties who use AI technologies or tools for academic, research, administrative, or operational purposes. AI tools include, but are not limited to:

- Machine learning applications
- Natural language processing tools
- AI-driven automation software
- Any systems that make decisions or recommendations based on algorithmic data processing

---

3. Definitions

- **Artificial Intelligence (AI):** Technologies that simulate human intelligence to perform tasks or support decision-making. This includes machine learning, natural language processing, and autonomous systems.
- **Acceptable Use:** Ethical and legal use of AI systems consistent with A-State policies and laws.
- **Data Privacy:** Proper handling of personal and sensitive data, including collection, storage, and sharing, in accordance with relevant regulations.

---

4. General Principles

All AI usage at A-State must adhere to the following principles:

- **Transparency and Accountability:**
  Users must disclose when AI is used for decision-making, content generation, grading, or other impactful processes.
- **Bias and Fairness:**
  AI tools must be implemented fairly. Users should actively mitigate biases that may affect individuals based on race, gender, age, or other protected characteristics.
- **Data Privacy and Security:**
  AI usage must comply with A-State data policies and applicable laws, especially those listed in Section 8.
- **Academic Integrity:**
  AI must not compromise academic honesty. Students must disclose AI use where required and follow the Academic Integrity Policy.
- **Informed Consent:**
  Individuals must be informed when their data is processed by AI systems, and explicit consent must be obtained when necessary.

---

5. Use of AI in Education

- **Faculty Responsibilities:**
  Faculty must use AI to enhance—not replace—traditional teaching. They must also disclose AI use in grading and educate students on ethical AI usage.
- **Student Responsibilities:**
  Students may use AI to support learning but must not use it to complete assignments or exams dishonestly.

---

6. Use of AI in Research

AI use in research should:

- Support (not replace) ethical research practices
- Comply with institutional research ethics and regulatory requirements

---

7. Use of AI in Administrative and Operational Functions

When AI is used in university operations (e.g., admissions, financial aid):

- The university must clearly disclose where and how AI is used
- Human oversight must be applied to AI decisions that affect individuals

---

8. Ethical and Legal Compliance

AI use must comply with relevant regulations, including but not limited to:

- **FERPA** (Family Educational Rights and Privacy Act)
- **GLBA** (Gramm-Leach-Bliley Act)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- Other applicable federal, state, or international laws such as:
  - **UK Data Protection Act 2018**
  - **EU GDPR**
  - **EU AI Act**
  - **China's Personal Information Protection Law**

Legal questions should be directed to the ASU System General Counsel's Office.

---

9. Prohibited Uses of AI

The following are not permitted:

- Using AI for academic dishonesty (e.g., cheating or plagiarism)
- Collecting or using personal data without authorization
- Discriminatory or biased use of AI
- AI surveillance without approval from A-State IT Security and Legal departments

---

10. Use of AI Assistant Guidelines

10.1 Overview

AI assistants, such as those integrated into Microsoft Teams or Zoom, can provide valuable support in meetings by generating summaries, action items, and transcripts. However, they are not appropriate for all settings and should only be used in meetings where their presence aligns with meeting objectives, privacy expectations, and institutional policy.

10.2 Risks to Consider

- **Privacy Concerns** – AI assistants record and process meeting content, which may include sensitive or confidential information.
- **Data Security** – Content may be stored in third-party systems depending on the AI service provider, potentially outside the institution's control.
- **Compliance** – Certain discussions (e.g., FERPA-, HIPAA-, or CJIS-protected data) must not be recorded or processed by AI assistants.
- **Informed Consent** – All participants should understand and agree to AI assistant use prior to recording or summarizing a meeting.
- **Legal Considerations** – Recorded discussions and summaries/transcripts may be subject to legal discovery in future litigation.

10.3 Guidance for Approved Use of AI Assistants

- AI assistants should never be enabled by default in recurring meetings or meeting templates.
- AI assistants may be used in Microsoft Teams meetings only when all participants provide explicit consent at the start of the meeting.
- The meeting organizer is responsible for announcing the AI assistant’s presence and its intended function (e.g., transcription, note-taking, summarization).
- Avoid enabling AI assistants in meetings that include confidential, legally protected, or sensitive data.
- Store and share AI-generated notes only in secure, approved A-State storage platforms (e.g., Microsoft OneDrive, SharePoint) and should only be shared with individuals who were part of the meeting.

10.4 General Guidance on Preventing AI Assistants from Joining Meetings

- In Microsoft Teams, review and adjust meeting options before the session to ensure that AI assistants are not automatically admitted.
- Disable transcription, recording, or meeting summarization features unless explicitly needed and approved.
- If an AI assistant joins unexpectedly, the meeting organizer should remove it immediately and verify settings before proceeding.

---

11. Compliance and Enforcement

Misuse of AI may result in disciplinary action per A-State's employee and student handbooks. The university may review AI usage to ensure institutional compliance, especially for licensed tools.

---

12. Review and Updates

These guidelines will be reviewed as AI technologies and regulations evolve. The IT Security Panel will monitor compliance and propose updates when necessary.

---

13. Contact Information

- **Security Inquiries:** security@astate.edu
- **Academic AI Use Questions:**
  Madeline Ragland, Assistant Vice Provost for Academic Student Services
  mprestidge@astate.edu

---

14. Approved AI Platforms

See **Appendix I** for A-State-approved AI platforms. All other tools must go through the standard **Software Purchase Request** process, including submission of a VPAT and HECVAT or ITS Security Questionnaire.

Use of **OpenAI** platforms such as **ChatGPT** or **DALL·E** is discouraged unless a **Business Associate Agreement (BAA)** is obtained.

Appendix I – Approved AI Platforms

The following AI tools meet A-State's compliance and data protection standards:

- **Microsoft Copilot** (Strongly Recommended)
  - Fully compliant with FERPA and HIPAA
- **ChatGPT Business** (requires minimum 2 license purchase by department)
- **Claude Pro** (Anthropic)
- **OtterAI**

While Microsoft Copilot is preferred due to its robust compliance standards, other listed tools are acceptable for use. OpenAI platforms (e.g., ChatGPT, DALL·E) are generally discouraged unless approved through a BAA.

Revision #10
Created 2025-06-02 18:09:47 UTC by Josh Breytspraak
Updated 2026-07-28 20:07:01 UTC by Jacob Weaver