Augusta University
Policy Library

Artificial Intelligence Policy
Policy Manager: Office of the Provost

POLICY STATEMENT

Artificial Intelligence (AI) tools and technologies can enhance university learning experiences, foster innovation in research, and improve administrative efficiency. However, it is crucial to ensure that AI is used responsibly and ethically to uphold the values of academic integrity, equity, and privacy. The Augusta University (AU) community is encouraged to use these tools responsibly, ensuring alignment with the university's values, safeguarding sensitive data, and complying with federal and state laws and regulations, as well as University System of Georgia (USG) and AU policies.

The intent of this policy is to provide general guidance on the use of AI at AU so that AU can leverage the use of AI as a tool while ensuring it continues to meet legal obligations and act in an ethical manner. The use of AI at AU should never compromise AU's core values or introduce undue risk to the organization. Rather, the use of AI at AU should be focused on improving business efficiencies and enhancing AU's ability to fulfill its mission. It is important to remember that AU is a state educational institution with collaborative research efforts and students around the globe. With this global span of users this policy is accordingly written to provide overarching guidance based on global standards for the use of AI. Users should be cognizant when using AI at AU that they think about the impacts of their decision to use AI, as the use of AI in some countries may not be permitted in others.

This policy establishes a framework for responsible, ethical, transparent, and appropriate AI use, while addressing risks like misuse and misalignment. It outlines best practices for protecting against unauthorized access, reducing security risks, and ensuring compliance with regulations. It also provides references to related AU policies and relevant guidance in AI contexts.

This policy applies to all faculty, staff, and students at the university and governs the use of AI in teaching, learning, research, administrative functions, and scholarly communication. Additionally, the university policy on AI applies to all members of the extended community (e.g., vendors, visitors) when engaged in activities at AU.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☒ Visitors
☐ Other:

Office of Legal Affairs Use Only
Executive Sponsor: EVP for Academic Affairs and Provost
Next Review: 8/2027

DEFINITIONS
These definitions apply to these terms as they are used in this policy:

1. **Artificial Intelligence (AI):** The term "artificial intelligence" or "AI" has the meaning outlined in United States Code 15 U.S.C. 9401(3): "The term 'artificial intelligence' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to-

a. perceive real and virtual environments.
b. abstract such perceptions into models through analysis in an automated manner; and
c. use model inference to formulate options for information or action."

2. **Generative AI:** Generative AI includes any machine-based tool designed to consider user questions, prompts, and other inputs (e.g., text, images, videos) to generate a human-like output (e.g., a response to a question, a written document, software code, or a product design). Generative AI includes both standalone offerings such as ChatGPT, Bard, Stable Diffusion, and offerings that are embedded in other software. Generative AI differs from traditional AI as Generative AI creates new content like text and images, whereas traditional AI (e.g. SAS, SPSS, STATS, etc) analyzes and interprets existing data for tasks like prediction and classification. Generative AI creates original content by learning patterns from existing data, posing potential risks. The term 'AI' used herein encompasses Generative AI (GAI).

3. **Sensitive Information** is information maintained by a USG organization that requires special precautions to protect from unauthorized use, access and disclosure guarding against improper information modification, loss or destruction. Sensitive information is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws but is not necessarily intended for public consumption.

4. **Confidential Data** encompasses information subject to limitations on accessibility and distribution, as dictated by legal and contractual obligations. This category includes data whose inappropriate use or disclosure could detrimentally affect the institution's mission accomplishment.

5. **AI Agent**: An AI agent is a system that uses artificial intelligence to autonomously perceive its environment, make decisions, and take actions to achieve specific goals—often through iterative reasoning, tool use, and adaptation based on feedback. Unlike simple chatbots that respond to single queries, agents can break down complex tasks into steps, use external tools, and adjust their approach based on results. Example: A customer service AI agent receiving a complaint about a delayed order might autonomously check the shipping database, identify the issue (warehouse backlog), draft an apology email with a discount code, update the customer's account notes, and escalate to a human supervisor if the delay exceeds company policy—all without human intervention at each step.

POLICY

1. **Guidelines for Use and Ethical Principles.** The following principles must be followed when considering using an AI system at AU:

a. Users are responsible for verifying the accuracy of AI-generated information and ensuring it is error-free and unbiased. AI systems are trained on data that may contain inherent bias. Users of these systems are responsible for reviewing any AI-produced content for bias or hallucinations and correcting it as necessary. Additionally, users must comply with copyright and intellectual property laws, avoid infringement, and guarantee that all content meets legal standards.

b. All AI-generated content must be thoroughly reviewed to evaluate such content for accuracy as well as general proofing and editing. AI-generated content should be viewed as a starting point, not the finished product.

c. Confidential, sensitive, regulated data or non-public AU information must never be put into an open AI system.

d. AU login credentials must not be provided to, or shared with, AI Agents without written authorization from the CIO.

e. The use of an AI system must be disclosed to capture institutional knowledge. For example, if AI is used to create code and included in a larger section of code, there must be documentation as to which code section is AI-derived and who reviewed it. Disclosure should be considered when using AI in much the same way as citing a source in writing.

f. The use of an AI system must comply with any terms of use or contractual limitations. Users should have all terms or use or contracts for AI systems reviewed by the Legal Department to ensure compliance with contractual obligations in using an AI system.

g. *Compliance with Data Privacy Laws, Regulations, and Policies*. AI users and tools must adhere to all applicable laws and regulations as well as USG and AU data policies. The collection and use of human-related data should be based on informed consent. AU employees may access sensitive data such as personnel records, student information, protected health information, intellectual property, and research data, but accessing AU data with or without authorization does not imply permission to use that data in AI models.

h. *Transparency in Data Collection and Usage.* In use of human-related data, AI users should adhere to ethical standards, regulations, policies, and safeguard the rights and privacy of human participants. For details on conducting research with human subjects, refer to AU's Human Research Program.

i. *Privacy and Confidentiality.* All data utilized in AI projects must be managed per the University's policies on data privacy. The user is responsible for determining whether privacy impact assessments need to be conducted by AU through its relevant offices. Personally identifiable information must be protected through stringent data collection practices and adherence to user permissions.

j. *Transparency in Decision-Making.* Users should explain how AI is used in decision-making. AI should not replace human-centered approaches or be used for automated decisions in university processes. Users who create content using artificial intelligence must clearly disclose the involvement of AI in the content creation process. Faculty who develop instructional resources using AI and build assignments anchored in AI shall acknowledge attribution.

k. Users may only transfer, disclose, upload, or share information in AI software or AI enabled software or tools that is permitted under AU policies, federal and state laws and regulations, and AU policies and guidelines.

l. With regard to the use of AI in academic activities, instructors and faculty should explicitly outline their AI use expectations for students, clearly defining the boundaries between acceptable and unacceptable uses. Students using AI must follow individual instructors' expectations outlined in teaching materials and the classroom. (See Academic Honesty Policy).

m. *Ethical Principles.* All users will adhere to ethical principles through use of AI, such as fairness/mitigation of bias, accountability, free from hallucinations, transparency, human oversight, accessibility, and safeguards against prompt injections. Accordingly, any use of an AI system at AU should conform to AU privacy and data policies.

2. **Procurement of AI tools/software.** Users seeking to purchase software or install on AU devices software or tools that use AI technology must follow the AU Procurement of Information Technology Policy, which employs the AU IT and Data Review Process to flag and categorize tools that utilize artificial intelligence capabilities and generate reports for periodic review, obtain vendor documentation and assurance of ethical compliance, and facilitate periodic audits of AI tools to assess adherence to ethical standards. All AI tools in use at AU are subject to annual cybersecurity reviews.

3. **Student Use of AI tools.** The Division of Enrollment & Student Affairs and the Division of Academic Affairs will ensure that students will be provided with AI literacy guidance in the Student Handbook and directed to augusta.edu/ai for additional context-specific resources and training. Course syllabi will provide course-specific expectations for acceptable use.

4. **Training.** Faculty, staff, and volunteers will be provided with AI literacy guidance in the Employee Handbook during onboarding and directed to augusta.edu/ai for additional context-specific resources and training. Annual compliance training for faculty and staff will include content specific to the use of AI, and specific departments or functions at AU may be directed to more training on the use of AI

systems and/or generative tools for the department or function.

5. **Research Use of AI tools.** Researchers are required to adhere to minimum disclosure standards for the use of AI in research and publications. All research using generative AI software or tools must be disclosed to IRB, AU AI governance committee and the AU Division of Sponsored programs before use.

6. **Reporting.** Any user aware of any conduct that may violate this policy has a responsibility to report it. Individuals are encouraged to make reports through established reporting processes and normal reporting relationships as detailed in the Policy on Reporting a Compliance or Ethics Concern. All reports of suspected misconduct or non-compliance will be investigated by Human Resources, Legal Counsel, or other appropriate parties. Unintended upload or sharing of sensitive data with an AI system or tool must be reported to Privacy immediately.

RESPONSIBILITIES

The President will appoint an AI governance committee co-chaired by the Provost (or designee) and the Chief Information Officer (CIO) to ensure ethical use of AI and compliance with regulatory requirements and policies and provide review and determination on any exception to this policy.

The AI Governance Committee will ensure that policies and procedures align with Artificial Intelligence Guidelines: A USG IT Handbook and that they are applied in accordance with the standards, procedures, and guidelines provided in the Academic & Student Affairs Handbook. The committee will also recommend revisions to this policy to align with updated regulatory requirements.

The Division of Information Technology will inventory AI tools, with review by the AI Governance Committee, with the required information in accordance with USG policies, to include but not limited to: Name, Vendor, AI Type, AI model type, description of how data interacts (institutional/student data), data storage and purpose of tool. IT will conduct periodic audits of AI tools to assess adherence to ethical standards including, but not limited to procurement and renewal reviews.

The Office of Academic Affairs and The Office of Student Affairs. The offices will develop and maintain guidance regarding the ethical use of AI for the academic environment. The offices will also develop and maintain guidance to ensure AI tools used in academic contexts comply with applicable laws, regulations, and industry standards; and ensure data used with AI tools is collected and processed in compliance with privacy laws (e.g., FERPA, GLBA, CCPA).

Office of Faculty Affairs. The Office of Faculty Affairs will ensure guidance is published and maintained for faculty on the ethical use of AI, specifically as it pertains to Faculty Affairs and production of scholarly communications.

Third-Party AI Vendors. All third-party AI vendors must provide documentation and assurance of ethical compliance during both the procurement and renewal processes. This includes:

- Certification of adherence to ethical AI principles
- Documentation of bias testing and mitigation strategies
- Transparency regarding data usage, storage, and retention practices
- Evidence of compliance with applicable privacy laws and regulations

The Office of Faculty Affairs will also guide the use of AI in producing scholarly communications, such as literature reviews, grant proposals, academic writing, and publishing, should include disclosures of use and a thorough review of the content generated by the AI tool to ensure accuracy and avoid including information that infringes on intellectual property or copyright. Authors should adhere to specific policies and guidance from funding agencies and publishers.

CONFLICT WITH BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA POLICIES. In the event of a conflict between this Policy and the official Policy of the Board of Regents of the University System of Georgia, the Board of Regents of the University System of Georgia's Policy shall prevail.

REFERENCES & SUPPORTING DOCUMENTS

- AU Artificial Intelligence Guidelines
- AU IT and Data Review Process
- USG Artificial Intelligence Guidelines: A USG IT Handbook Companion Guide
- GTA Standard: Artificial Intelligence Responsible Use (SS-23-002)
- GTA Guidance: 5 Guiding Principles
- GTA AI Selection Guidance
- Georgia Open Records Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Educational Records Protected Under the Family Educational Rights and Privacy Act (FERPA)
- GLBA (Gramm-Leach-Bliley Act)
- AI Export Controls of Regulated Data (Regulations 3A090 and 4A090)
- The IIA's Artificial Intelligence Auditing Framework
- NIST AI 100-1 Artificial Intelligence Risk Management Framework

RELATED POLICIES

- Acceptable Use of Information Technology
- BOR Policy: 6.28 Artificial Intelligence in Academic Contexts
- USG Policies
- Procurement of Information Technology Policy
- Academic Honesty Policy

- Sanctions for Privacy and Cybersecurity Violations
- Privacy of Health Information
- Data Management and Classification Policy
- Record Retention Policy
- Policy on Reporting a Compliance or Ethics Concern

REVIEW PERIOD
This policy will be subject to annual review.

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/29/2026

President, Augusta University Date: 7/7/2026