



Eastern Kentucky University

Policy and Regulation Library

Administrative Regulation: 11.##

Responsible Office(s): Information Technology

Effective:

Next Review Date: Fall 2028

Administrative Regulation: 11.[ADR NUMBER] Use of Artificial Intelligence in the Workplace DRAFT

Statement

The purpose of this policy is to provide guidance on the usage of Artificial Intelligence (AI) tools in the workplace at Eastern Kentucky University ("University" or "EKU"). These tools can be effective at saving time and improving productivity for a wide range of tasks, but they also introduce potential issues for data security and ethics violations. This policy applies when AI tools are used to perform, or assist in the performance of, any work-related activities and applies regardless of the location of AI users at the time they use AI tools, and regardless of whether the AI tools are used on University devices, personal devices, or third-party devices.

AI tools use technologies that allow for machine learning, pattern recognition and prediction, and natural language interaction that resemble human thought. AI tools include generative systems such as large language models and image generators, as well as other categories like text-to-speech, speech-to-text, spelling/grammar checks, image and video recognition or manipulation, robotics, and language enhancement technologies. These new tools can be highly effective, but this regulation seeks to ensure that they are used in compliance with all laws, regulations, and policies to respect privacy, confidentiality, data security, and ethics.

This policy should be read in accordance with [Policy 1.2.1 Code of Ethics](#), Academic Regulation [4.1.3 Academic Integrity](#), Administrative Regulations [11.2.1 Acceptable Use of Information Technology Resources](#) and [11.2.4 Information Security](#), and any other applicable university policies.

Entities Affected

All University Community Members, students, faculty, and staff, as well as anyone doing business for or with the University.

Procedures

I. Confidential Information & PII

Data that is entered into AI tools may be stored, reprocessed, and made accessible to the tool's makers, other users, or outside parties, including through legal processes such as litigation or discovery. Therefore, users should treat all information submitted to an AI tool as potentially public. Extreme caution must be taken if you use any AI tools, including vendor-created AI tools embedded in programs or software with which the University has a contractual agreement. Use of University-contracted tools with AI functionality should follow FERPA and Data Trustees protocols as well as procedures outlined below. University Community Members cannot enter or upload any Confidential Information or Personally Identifiable Information (PII) into vendor-created AI tools except when permitted by validated contract language and security controls.

Public AI tools shall be classified and treated distinctly from University-contracted tools. Public AI tools are not subject to institutional security controls, data governance oversight, or contractual safeguards. Accordingly, public AI tools shall not be used to process, transmit, or store University data, including, but not limited to, confidential, proprietary, or Personally Identifiable Information (PII). A list of current ECU University-contracted tools can be found on the [ECU Artificial Intelligence Guidance Webpage](#).

University Community Members may only use University-contracted tools or public AI tools that have been vetted for use by the University's IT Department. To reduce the risk of unintentional disclosure, the following restrictions and guidelines apply:

- A. No protected data subject to government statute or regulation (e.g., HIPAA, FERPA, GLBA, PCI) may be entered or uploaded into any AI tool, unless the tool is University-contracted and explicitly approved for such use under its vendor agreement and institutional review.
- B. No Personally Identifiable Information (PII) about students or employees may be entered or uploaded, including student information subject to an active Confidentiality Flag.
- C. No confidential financial data may be entered, including account numbers, credit card information, payroll details, or other sensitive institutional finance records.
- D. No University Confidential Information may be entered or uploaded into any AI tool.
- E. University data that is publicly available or intended for public dissemination (e.g. published course catalogs, academic calendars, policies, press releases, etc.), may be entered into AI tools.
- F. Questions, prompts, and responses should be anonymized before being entered into AI tools.

II. Ethical Use for AI Tools

- A. AI tools must not be used to violate federal, state, or local laws.
- B. AI tools must not be used to create, distribute, or assist in the development of malware, phishing attempts, spam, or other forms of cyber fraud or scams.
- C. AI tools must not be used to knowingly infringe upon copyrights, patents, trade secrets, license agreements, or other intellectual property protections. Users are responsible for ensuring that both inputs and outputs comply with applicable laws and contract terms.
- D. AI tools must not be used to violate sponsor requirements or academic integrity standards. AI tools must not be used in research or sponsored projects in ways that violate funding agency requirements, grant terms and conditions, or academic integrity standards.
- E. University researchers are responsible for ensuring that any use of AI tools in research complies with Institutional Review Board (IRB) requirements and related guidance.
- F. AI tools must not be used to circumvent or violate University policies, rules, or guidelines.
- G. AI tools must not be used in any manner inconsistent with responsible, ethical, or professional conduct, or that may otherwise compromise the integrity or reputation of the University.
- H. AI tools must not be used to harass, stalk, defame, or discriminate against others.
- I. AI-generated output should be carefully reviewed for accuracy, bias, and appropriateness before being included in official documents, communications, or public-facing materials.
- J. AI-generated output created using AI tools should also be reviewed to ensure that Confidential Information, Personally Identifiable Information (PII), or other protected data has been removed prior to use in official documents, communications, or public-facing materials.

III. Limitations of AI Tools

- A. Users of AI tools should be aware of the following limitations:
 - 1. AI tools may generate inaccurate or fabricated content, including false citations, misinterpreted data, or misleading summaries. This phenomenon is commonly referred to as a “hallucination.”
 - 2. AI tools may reflect or amplify biases present in their training data.
- B. AI tools generally should not be relied upon to answer factual or evaluative questions, as they often reinforce the assumptions, opinions, or biases embedded in the user’s prompt. This limitation does not apply to approved, domain-specific AI tools, such as retrieval-augmented generation (RAG)

systems, that are designed to return evidence-based responses with verifiable citations.

- C. Users should verify AI-generated content using appropriate, independent sources, and critically evaluate its reliability, appropriateness, and accuracy before presenting it in any instructional, operational, or public-facing context.

IV. Permissible AI Tools

- A. AI tools must undergo a security and privacy review by the University's IT Department prior to adoption. A list of approved AI tools in these products and services will be published on the [EKU Artificial Intelligence Guidance Webpage](#).
- B. Due to unresolved concerns regarding data privacy, security compliance, and academic integrity, the use of unapproved AI tools is highly discouraged at ECU. A list of approved tools may be found on the [EKU Artificial Intelligence Guidance Webpage](#).

Definitions

- **AI Tool:** Any software, platform, or service that uses artificial intelligence ("AI") technologies, including machine learning algorithms, to generate, process, analyze, or interact with content. This includes, but is not limited to, generative AI systems (e.g., large language models, image generators), AI-enhanced applications (e.g., text prediction, summarization, translation), and tools used for speech, image, video, or data recognition and manipulation. AI tools may be embedded in existing software or accessed as standalone applications.
- **Confidential Information:** Personally Identifiable Information (PII) or sensitive information including, but not limited to, social security numbers, ECU identification numbers, student grade information, sensitive reports, medical records, military records, student disciplinary records, personnel records, and counseling and disability records.
- **University-Contracted AI Tool:** An AI tool that has been procured, contracted, or otherwise acquired by the University under the procedures set forth in Administrative Regulation [6.2.2ADR, Contract Review, Approval, and Execution](#).
- **FERPA Data:** Data or information contained within student educational records which is not otherwise deemed directory information by the institution. ECU has designated the following as non-public, FERPA-protected information, for example:
 - Social Security Number
 - GPA
 - Grades

- Academic history
- Student schedule
- Academic standing
- Student ID
- Residence hall room number
- **Personally Identifiable Information (PII):** An individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements
 - An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
 - A Social Security Number;
 - A taxpayer identification number that incorporates a Social Security number;
 - A driver's license number, state identification card number, or other individual identification number issued by any agency;
 - A passport number or other identification number issued by the United States government; or
 - Individually identifiable health information as defined in 45 C.F.R sec 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C sec 1232g (KRS 61.931 (6) (a-f))
- **Public AI Tool:** An AI tool that is available for general public use and has not been procured, licensed, or approved by the University. These tools have not undergone institutional review and do not offer University-approved data protections or contractual safeguards. Public AI tools are typically accessed through personal or non-University-contracted accounts and are not authorized for processing University data or connecting to institutional systems.
- **Retrieval-Augmented Generation (RAG) System:** An artificial intelligence (AI) system that combines a language model with an external knowledge retrieval mechanism. Instead of relying solely on pre-trained data, RAG systems retrieve relevant documents or records from a trusted source in real time to generate responses grounded in verifiable information. Approved RAG systems may be used to support evidence-based tasks where citation, traceability, and contextual accuracy are required.
- **Unapproved AI Tool:** An AI tool that has not been formally reviewed or approved by the University's Information Technology Department for institutional use. This includes both public tools and commercially available tools that lack official University authorization and may present risks related to data privacy, security, academic integrity, or University policy compliance.

- **University Community Member:** All students, faculty, and staff, as well as anyone doing business for or with the University
- **Vendor-Created AI Tool:** An AI tool or feature embedded within software or digital services that have been licensed or procured by the University. These tools may include generative capabilities such as large language models (LLMs), image generation, or predictive analytics. This definition does not include standard automation features such as spellcheck, grammar correction, autocomplete, or macros unless they incorporate machine learning or natural language generation. The University may periodically review embedded features to determine whether they meet the threshold for AI classification under this policy.

Statutory or Regulatory References

- Family Education Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232g
- Health Insurance Portability and Accountability Act (“HIPAA”), 42 U.S.C. § 1320d-2

Relevant Links

- [EKU Artificial Intelligence Guidance Webpage](#)
- [EKU Institutional Review Board \(IRB\) Webpage](#)

Policy Adoption Review and Approval

Regulation Issued

Date
X

Entity
X

Action
X