Using Generative AI with University-Owned Records and Data Policy

Chapter ????

Created ??/??/????

Revised ??/??/????

Table of Contents

.010 Statement

To comply with the State of Kansas Generative Artificial Intelligence Policy and to mitigate risk to the University, this Policy provides requirements for the use of Generative Artificial Intelligence ("AI") (e.g., ChatGPT, Microsoft Copilot, OpenAI, etc.) to employees of Kansas State University ("University" "KSU") and those performing work and/or services for the University ("service providers and contractors"). Generative AI, a facet of artificial intelligence, demonstrates the ability to create diverse content such as art, music, and text through the utilization of models trained on extensive datasets.

This Policy is used to define the controls when using Generative AI, and is intended to mitigate the following risks to the University:

- Introduction of viruses and malware to the network.
- Loss or theft of intellectual property owned by the university.
- Damage to the university's reputation.

The purpose of this Policy is to regulate the use of Generative AI with University-owned records and data within the employment sector, while acknowledging the dynamic nature and constant evolution of Generative AI. This Policy emphasizes the need for annual updates to accommodate the evolving landscape of Generative AI and ensure its responsible integration within the University's employment field.

This policy falls under the authority of *(TBD)* office(s). In collaboration with critical stakeholders including Records Management, Data Governance, General Counsel, and Institutional research, *(TBD)* office(s) oversees the annual review, updating, and implementation of the policy.

.020 Scope and Applicability

This Policy shall serve as the primary governing document for usage of Generative AI technology for University-owned records and data.

This Policy applies to all employees of the University and service providers and contractors performing work and/or services performed for the University using, creating, and working with University records and data.

This Policy applies to all business use cases involving the University, including but not limited to:

- development of software code,
- written documentation (i.e., policy, legislation, or regulations) and correspondence (such as memorandums, letters, text messages, and emails),
- institutional research,
- summarizing and proofreading documents,
- making business decisions that impact short-term or long-term activities or policies and procedures,
- student recruitment and admissions,
- faculty recruitment and hiring,
- student and faculty publications.

Additionally, this Policy does not apply to the use of Generative AI for purely personal reasons. However, use of Generative AI for personal reasons should not occur on University-issued devices and should not use, rely on, or be populated with the University's records or data.

.030 Policy

Whether users should use Generative AI in the performance of their responsibilities is dependent on the specific use of Generative AI. The issues raised with the use of Generative AI to assist with menial tasks (e.g., proofreading non-protective written content) are much different than skilled tasks (e.g., drafting outward-facing University publications). Users must exercise good and sound judgment, consistent with the guidelines in this Policy, prior to using Generative AI for University purposes.

Responsibilities

Responses generated from Generative AI outputs shall be reviewed by knowledgeable human operators for accuracy, appropriateness, legality, privacy, and security before being acted upon or disseminated.

Users should be aware that the use of Generative AI may create University records that fall under the Kansas Opens Record Act. Chapter 3060 provides University guidelines for this Act.

Employees shall ensure that service providers and contractors align with the University's principles on the ethical use of AI, which includes transparency in AI decision-making processes, fairness, non-discrimination, and accountability in case of errors or biases. Furthermore, service providers and contractors employing Generative AI technologies must adhere to the University's data protection policies and comply with relevant legal regulations (including the GDPR and FERPA).

If service providers and contractors utilize tools that incorporate Generative AI, then such service providers and contractors must disclose in their contracts with the University that their tools incorporate Generative AI technologies, detailing how these technologies are used and the safeguards in place to protect this data. This information should be clearly communicated to the University prior to the acquisition or renewal of any service contract.

Where service providers and contractors are providing a service to KSU with AI capabilities but are not using KSU-owned data, the service providers and contractors must disclose in their contracts the utilization of Generative AI or integrations with Generative AI platforms. Moreover, in cases where service providers, vendors, or contractors utilize AI capabilities while handling KSU-owned data, their contracts must explicitly state the use of Generative AI or integrations with Generative AI platforms. Furthermore, they are required to obtain pre-approval from the Data Governance Steward Committee, which may seek guidance from the Data Governance Steering Committee as needed.

.040 Restrictions

The University firmly restricts the use of unaligned or intentionally misaligned Generative AI models in operations or any other activities associated with the University. There are limited scenarios where engagement with an unaligned model is justified by a legitimate business need. Such use must aim to enhance the University's understanding, readiness, and resilience against potential threats, without contributing to the propagation of harmful content or biases. Prior approval from the Data Governance Steward Committee, with the option to seek guidance from the Data Governance Steering Committee as needed, is required for any proposed utilization of an unaligned AI model.

The use of Generative AI may not breach the University's obligations to comply with applicable state and federal laws and regulations, as well as University and Kansas State Board of Regents policies. This includes the University's obligations regarding Protected Information.

The University restricts the following uses of Generative AI:

- Users shall not enter any Protected Information into Generative AI that is not an approved process or system by Kansas State University. Exceptions to this bullet will follow the previously mentioned Review Group process.

- Materials that go against Copyright and Artificial Intelligence | U.S. Copyright Office and Intellectual Property (k-state.edu) laws and University policies.

- Users shall not use Generative AI to generate or enable content that is discriminatory, defamatory, illegal, or in violation of applicable University policy, laws, or regulations.

- Users shall not use Generative AI to upload any data that could be used to help create or carry out malware, spam and phishing campaigns or other cyber scams.

- Responses generated from Generative AI shall not:
  - be used verbatim,
  - be assumed to be truthful, credible, or accurate,
  - be used to issue official statements (i.e., policy, legislation, or regulations),
  - be used to break the University's Principles of Community.

.050 Risks, Liabilities, Disclaimers

Employees who elect to participate in the mismanagement of Generative AI accept and understand the following risks, liabilities, and disclaimers:

- Persons violating this Policy may be held personally liable for resulting damages and civil or criminal charges. Kansas State University will comply with any applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies.

- Compliance with this Policy is required, and employees who fail to follow it may be subject to sanctions under applicable University policies, including written reprimand and in serious cases, termination for cause.

.060 Transparency

The use of Generative AI should be transparent. For example, if creating a document, data, and/or information using Generative AI, its use should be disclosed and made clear on the document.

.070 Definitions

The following definitions are relevant to this Policy:

Generative AI
A form of artificial intelligence that utilizes algorithms and models trained on large datasets to generate new creative content, ranging from text, images, and music to other data types, by learning patterns and structures from the data.

Protected Information
Any data, including altered or redacted data, that includes but is not limited to:

- Personally identifiable information protected by FERPA, such as:
  - Social security numbers
  - University card ID photos and ID numbers,
  - Coursework produced by students,
  - Student grades,
  - Student disability information,
  - Student disciplinary records.

- Personally identifiable employee data or information related to employees and their performance.

- Health information protected by HIPAA.

- Information protected by the General Data Protection Regulation (GDPR).

Records
Information the University creates and maintains while doing business. Records can be in any media, including paper, magnetic tape, and optical disks. Work-related records, including emails, that Users produce in their homes and on their personal home computers are still the property of the University.

Unaligned
A Generative AI platform lacking a contractual agreement or vendor status with the University. Includes encompassing free, in-house, subscription-based platforms utilized by users, etc.

University Community
Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing University network services, and other authorized users.

Users
Persons who have access to University systems, data, and records. This includes University employees, student workers, contractors, contingent workers, agents, consultants, vendors, service providers, suppliers, and other third parties.

.080 Compliance

The University reserves the right to audit networks and systems periodically to ensure compliance with this Policy. Instances of non-compliance must be presented and reviewed and approved by the Director of Information Security, or equivalent officer.

All breaches of information security, actual or suspected, must be reported to and investigated by the Director of Information Security, or equivalent officer.

Those who violate security policies, standards, or security procedures are subject to disciplinary action up to and including loss of computer access and appropriate disciplinary actions as determined by the University.

.090 Related Policies, Standards, and Regulations

- PPM 3060: Kansas Opens Record Act
- PPM 3090: Retention of Records
- PPM 3420: Information Technology Usage Policy
- PPM 3433: Data Classification and Security Policy
- PPM 7095: Intellectual Property
- Use of University Mobile Devices, Personal Devices, and Accounts Policy

- KANSAS PPM 8200: Generative Artificial Intelligence Policy
- KSU Institutional Data Policy
- Controlled Unclassified Information (CUI)
- FERPA (k-state.edu)
- HIPAA Home | HHS.gov
- Generative Artificial Intelligence and Copyright Law
- Data Usage Policy - (In-process)
- Acceptable Use Policy - (In-process)