

# Siena University

## Institutional Use of Generative and Agentic Artificial Intelligence: Privacy, Security, and Compliance

### UNIVERSITY POLICY

<b>Policy Title:</b>	<b>Institutional Use of Generative and Agentic Artificial Intelligence: Privacy, Security, and Compliance</b>
<b>Type or category of Policy:</b>	<b>University Policy</b>
<b>Approval Authority:</b>	<b>The Provost and Senior Vice President</b>
<b>Responsible Executive:</b>	<b>The Provost and Senior Vice President</b>
<b>Responsible Office:</b>	<b>Chief Information Officer within Information Technology Services</b>
<b>Owner Contact:</b>	Angelo Santabarbara, <b>Chief Information Officer</b> <a href="mailto:asantabarbara@siena.edu">asantabarbara@siena.edu</a> 518-782-6996
<b>Reviewed By:</b>	<b>Academic Affairs</b>
<b>Reviewed Date:</b>	<b>February 5, 2026</b>
<b>Last Revised and Effective Date of Revision:</b>	

## Reason for Policy

Siena University supports the responsible and ethical use of Artificial Intelligence (AI) tools, including generative and agentic AI systems and other emerging or future AI-enabled technologies, to enhance learning, teaching, research, and administrative operations. All members of the Siena community are expected to use AI technologies in ways that align with federal, state, local, and international laws and regulations, as well as all University policies, including but not limited to the Acceptable Use Policy and Data Classification Policy.

## Scope of the Policy: Entities or Individuals affected by this policy

- All members of the Siena University community
- Volunteers, visitors, individuals employed by contractors on campus (ABM, AVI, St. Peter's, Friary, Bookstore, ROTC employees, etc).
- Anyone granted access to Siena University data

## Definitions

**Generative AI** is a general term for artificial intelligence designed to consider user questions, prompts, and other inputs (e.g., text, images, videos) to generate synthetic, human-like content (e.g., a response to a question, a written document, software code, or a product design). Generative AI includes both standalone offerings, and offerings that are embedded in other software.

**Agentic AI** refers to AI systems that are capable of initiating actions, making decisions, executing tasks, interacting with other systems, or acting on behalf of a user with limited or no direct human intervention.

## The Official Policy

### 1. Privacy and Data Protection

All data shared with AI systems, including data used for model training, tuning, retraining, or evaluation, must comply with Siena's existing privacy and information security policies. Data should only be processed, transmitted, or used for training purposes through University approved and licensed AI platforms that have been vetted for compliance, security controls, and contractual protections.

Users must ensure that no confidential, restricted, personally identifiable, or otherwise sensitive University data is entered into, used to train, or retained by public or non-approved AI platforms.

This includes, but is not limited to:

- Student records, grades, or personally identifiable information (PII) as defined under FERPA;
- Confidential employee information or human resources data;

- Financial, health, or research data governed by institutional, state, or federal regulations (e.g., HIPAA, GLBA, or IRB requirements);
- Any proprietary or internal sensitive University information, including non-public operational, financial, technical, or strategic data, internal communications, unpublished research, and any data classified as confidential or restricted by University policy.

Special care must be taken when configuring or enabling agentic AI systems to ensure they do not retain, infer, transmit, or act upon sensitive University data beyond their approved scope.

## **2. Security and Approved Use**

Use of generative and agentic AI must occur within secure, institutionally managed and/or contracted environments. Publicly available AI tools (e.g., open web-based models and AI-enabled wearable devices, browser extensions, mobile applications, and voice activated devices), including agentic systems, may only be used with non-sensitive, de-identified, or publicly available data.

Agentic AI systems that are capable of executing actions, accessing systems, initiating workflows, or integrating with University resources must not be enabled, deployed, or used without explicit institutional approval and appropriate safeguards, including authentication controls, logging, auditability, and defined limits on autonomy.

Siena University may provide institutionally licensed AI tools that have been reviewed by Information Security and are covered by contract to include enhanced privacy, audit, and data protection controls. Users are required to use these approved platforms when conducting University business, research, or instruction involving sensitive, confidential and non-public University data. Users should also be aware that their use of non-licensed ancillary systems (e.g. GitHub, Box, etc.) whether independently or in conjunction with an AI platform or agentic AI workflow, may put institutional data and systems at risk.

## **3. Compliance and Legal Considerations**

All use of AI tools must comply with applicable legal and regulatory requirements, including data protection, intellectual property, and accessibility laws. Users must:

- Follow all vendor licensing agreements and usage terms for AI tools approved by Siena University;
- Ensure AI-assisted or AI-initiated outputs and actions do not violate copyright, confidentiality, security, or ethical guidelines;
- Understand that institutional and legal responsibility rests with the user for any misuse, non-compliant disclosure of data, or unauthorized actions taken by AI systems acting on their behalf.

## **4. Ownership and Intellectual Property**

Content, data, and intellectual property produced using AI tools within Siena's licensed environments remain subject to existing University policies on data ownership and intellectual property. Outputs generated or actions taken through AI systems, including agentic AI, are not automatically proprietary to the AI provider. The University retains rights over institutional data, and users retain appropriate rights to their academic or creative work, consistent with Siena's intellectual property policy. The use of non-institutionally licensed AI environments does not afford these protections.

## **5. Accountability**

Each member of the Siena community is responsible for safeguarding University data and systems and for ensuring that any AI-related activity (including the configuration, delegation or oversight of agentic AI) complies with Siena's standards for data privacy, security, integrity, and ethical use. Users remain accountable for decisions, outputs, and actions taken by AI systems operating on their behalf. Violations of this policy may result in the revocation of access privileges and/or disciplinary action as outlined in the Acceptable Use Policy.

## **6. Enforcement of Policy**

Violations will normally be handled through the University disciplinary procedures applicable to the relevant user. Violation of this policy or any of its components therein carry sanctions which may include, but are not limited to, temporary or permanent suspension of account access up to termination of employment or suspension of enrollment. However, the University may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the University or other computing resources or to protect the University from liability.

## **7. Exceptions**

Exceptions may be granted by the Chief Information Officer (CIO) in limited circumstances based upon the needs of the University and upon the requestor's written justification. If required, the CIO may request review and approval by the University's Legal Counsel and/or Risk Officer.

## **Resources**

Acceptable Use Policy

<https://www.siena.edu/files/resources/acceptable-use-policy.pdf>

Copyright Ownership Policy

<https://www.siena.edu/files/resources/copyright-ownership.pdf>

Copyright Usage and Compliance Policy

<https://www.siena.edu/files/resources/copyright-usage-and-compliance.pdf>

Data Classification Policy

<https://www.siena.edu/files/resources/siena-college-data-classification-policy.pdf>

Information Regarding the Use, Distribution, and Sharing of Copyrighted Works Policy

<https://www.siena.edu/files/resources/information-regarding-the-use-distribution-and-sha.pdf>

Patent Ownership and Management Policy

<https://www.siena.edu/files/resources/patent-ownership-and-management-policy.pdf>

**Adopted: February 5, 2026**

**Reviewed:**

**Revised:**