William Paterson University Policy
University Policy

SUBJECT:	University Policy			**TITLE:**	Generative AI Policy and Guidelines for Employees		
CATEGORY: Check One	**Board of Trustees** ☐	**University** X		**Functional** ☐		**School/Unit** ☐	
Responsible Executive:	President and Cabinet Members			**Responsible Office:**	Information Technology		
CODING:	00-01-80	**ADOPTED:**		3/19/2025	**AMENDED:**		
				LAST REVIEWED: xx/xx/xx			

I. PURPOSE

This policy governs William Paterson University faculty, staff, and administrators' use of Generative Artificial Intelligence (AI) related to official work conducted for the University. This Policy and Guidelines document seeks to empower William Paterson University's staff and administration by providing guidelines for effective, secure, ethical, and innovative use of AI technologies in University operations.

This policy applies when AI tools are used to perform, or assist in the performance of, any work-related activities. This Policy 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. (From https://www.stjohns.edu/my-st-johns/human-resources/policy-1038-artificial-intelligence-workplace)

The guidelines below are intended to complement existing University policies. Any use of AI at William Paterson should also ensure that all University policies (including those on appropriate technology use, data privacy and protection, and others) are understood and taken into consideration. Please note that a second AI policy, AI: Use of Generative Artificial Intelligence in Student Academic Coursework, covers academic integrity and other issues pertaining to teaching and learning at William Paterson. The academic policy applies to anyone teaching courses, whether faculty, staff, or administrators.

This policy addresses William Paterson's need to safeguard University data by requiring that no protected data be entered into any AI Chats such as Microsoft Copilot and ChatGPT. Fully anonymized data may be entered into AI Chat tools. Should AI be embedded in a software platform in use or being considered at William Paterson, the software must be checked for security and approved by IT before any protected data is entered. Note: "AI" in this document stands for "Generative AI,"

II. ACCOUNTABILITY

While the Information Technology Department provides Generative AI tools, numerous free and paid AI tools are available and easily accessed on the Internet and through App stores. Therefore, all employees are responsible for the security of protected data in their use of Generative AI. With the proliferation of AI mechanisms into more and more platforms, applications, and the core systems of our computers, smart phones, and smart devices, it is important for all employees to recognize the rapid growth of AI and apply this policy and utilization guidelines to the many varied, and rapidly expanding applications, devices, and uses.

III. APPLICABILITY

All University employees must adhere to existing data security policies, laws, and regulations when using AI.

This policy is also applicable to all faculty, staff, administrators and other authorized users of University accounts, technology software and hardware, and AI use on personal or third party devices when conducting official University business.

IV. DEFINITION(S) (optional)

Generative Artificial Intelligence (AI) is a system of algorithms or computer processes that can create novel output in text, images or other media based on user prompts. These systems are created by programmers who train them on large sets of data. The AI learns by finding patterns in the data and can then provide novel outputs to users' queries based on its findings.

Generative AI systems are distinguished from other AI systems by their ability to create novel output. For example, predictive AI systems on smartphones can suggest a short, common response to an email by analyzing the text received and drawing from a pool of common responses. Generative AI systems like ChatGPT, which employs a Large Language Model, go a step further to provide new information for users based on their questions or requests.

Text-based generative AI systems are based on large language model (LLMs)s, which are huge probabilistic algorithms for drawing upon a corpus of text to predict likely sequences of words. Other generative AI systems may be based on images or sounds as well. (Source - https://www.nnlm.gov/guides/data-thesaurus/generative-artificial-intelligence)

V. BACKGROUND

Since the release of ChatGPT in 2022, widespread use of new tools identified as AI, more specifically generative AI, present powerful new ways of synthesizing information from the Internet and providing a vast amount of information in natural language formats using LLMs (large language models,). This technology has transformed the way people write, interact, research, create, and study.

AI, however, goes far beyond the chat interfaces popularized by OpenAI, ChatGPT, Microsoft Bing, Google Gemini, Meta AI, and others. AI systems are also embedded in many existing software platforms, as well as the voice recognition systems of Apple's Siri and Amazon Alexa. They are used in search algorithms in Google and Bing, they generate recommendations on streaming platforms, such as Netflix, YouTube, and Spotify. In addition to text and translation in hundreds of languages, including coding languages, AI generative tools are widely available to create images, music and musical scores, video, and audio including spoken voice content.

Along with the benefits of AI, the issue of data security has become more important than ever. This policy addresses William Paterson's need to safeguard University data by requiring that no protected data be entered into any AI Chats such as Microsoft Copilot and ChatGPT. Fully anonymized data may be entered into AI Chat tools. Should AI be embedded in a software platform in use or being considered at William Paterson, the software must be checked for security and approved by IT before any protected data is entered.

VI. REFERENCE(S)

Please see these related University policies:

- Electronic Recording of Lectures and Materials
- Technology Services and Resources
- AI: Use of Generative Artificial Intelligence in Student Academic Coursework

VII. POLICY

A. Requirements

As University employees, all faculty, staff, and other authorized users of William Paterson accounts, technology software and hardware, and AI use on personal and third party devices when conducting official University business will act responsibly and ethically in their use of Generative AI tools. For the purposes of this policy, Generative AI tools, whether stand-along or integrated into software. This Policy applies to Generative AI tools such as Microsoft Copilot ChatGPT, etc., as well as software platforms that have added AI, especially to process data, Generally, protected data as listed below should not be entered into these software platforms. If AI additions to software platforms would be

useful operationally, IT must verify whether appropriate security safeguards are in place before such data is entered.

B. Responsibilities

William Paterson reserves the right to monitor all employee interactions with AI tools for the purpose of ensuring compliance with this policy.

- Data Privacy

  Under no circumstances should any protected data (HIPPA, FERPA, etc.) be entered into any AI Chat, whether Microsoft Copilot, which WP has access to under our Microsoft subscription, or any other tools such as ChatGPT, Gemini, etc. Fully anonymized data may be entered into AI Chat tools. William Paterson employees and individuals with access to University data must ensure that all AI use complies with federal, state and local laws and regulations relating to data privacy. These laws include but are not limited to the following:

  - Family Educational Rights and Privacy Act (FERPA): AI must not process student education records.
  - Health Insurance Portability and Accountability Act(HIPAA): AI must not process medical records or health data.
  - Copyright Law: AI-generated content must not infringe on intellectual property rights.
  - General Data Protection Regulation (GDPR): Sensitive information (e.g., personally identifiable information, personnel data, health records, financial data) must not be entered into any AI tools, including Microsoft Copilot.
  - Gramm-Leach-Bliley Act (GLB): Student financial information obtained electronically or on paper while doing business with a student should not be entered into AI.
  - NJ-OIT: As a public institution, the University is required by New Jersey State law to comply with the policies and standards of the New Jersey State Office of Information Technology (OIT) as applicable to institutions of higher education.

- Internal Violations

  - William Paterson employees who violate any part of this policy will be subject to discipline according to HR disciplinary processes.
  - William Paterson AI users should contact Human Resources immediately if they become aware of an existing or potential violation of this Policy and should contact Information Technology via the Helpdesk regarding any existing or potential breach of data privacy or security related to the use of AI in the workplace. (Adapted from https://www.stjohns.edu/my-st-johns/human-resources/policy-1038-artificial-intelligence-workplace)
  - External Violations - Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

C. Enforcement:

Vulnerability Assessment: Information Technology is responsible for evaluating AI systems regularly for vulnerabilities and potential risks to avoid issues like data leaks or manipulation. As with all software purchases, any employee considering purchase or implementation of AI tools beyond individual use must submit information to IT for evaluation and approval.

VIII. PROCEDURE(S) (optional)

(This section is used to describe the actions to be taken by the various individuals in accomplishing a task, operation, or transaction, referenced in the Requirements section.)

IX. EXHIBIT(S) (optional)

(This section includes forms, illustrations, bibliographies and reference information.)

By Direction of the President and Cabinet:

Date

_____

(Title of Executive or Vice President(s) whose area of responsibility the policy covers.)
Gamin Bartle, CIO