Title:	**Guidelines for Generative Artificial Intelligence (GenAI)**
Issuing Authority:	**Office of the President**
Responsible Officer:	**Vice President for Information Technology**
Effective Date:	**July 24, 2024**
Reviewing Offices:	**Office of Information Technology Services**

Scope

This document provides guidelines for using Generative Artificial Intelligence (GenAI) technologies,[1] Including when they should and should not be used within the Temple University environment. As a university dedicated to exchanging ideas, distributing knowledge, and fostering innovation, we must embrace GenAI carefully and responsibly.

Publicly available GenAI tools such as ChatGPT, Google Gemini, Perplexity, Poe, and Microsoft CoPilot have gained tremendous visibility over the past year. They are used by individuals for teaching, learning, completing work tasks, and conducting research but may lack security and data regulation compliance features. Consequently, when using public GenAI tools, do not input or upload confidential, sensitive, or restricted research data as detailed below under "Principles."

Additionally, as with any use of software, Temple University needs the ability to verify the security posture of these applications/third-party tools. Temple needs to control what data these tools collect and how that data is managed and protected. All software purchased or accessed must go through the Pre-Approval Purchasing Process.

Please adhere to the following guidelines, which align with Temple's data, privacy, compliance, research, and security policies.

- **Confidentiality and Privacy**: Data shared with GenAI tools may be used or stored in ways that expose institutional, research, grant, or contract data (including, but not limited to, personally identifiable information (PII), Protected Health Information (PHI), institutional defined sensitive data, student data as defined under FERPA, and research data with export control restrictions) to third parties. Do not store or use data in any GenAI tool where confidentiality and/or privacy may be compromised. Public data may be used and retained within any GenAI application. Note that *incognito* features in certain AI applications do not guarantee confidentiality and privacy. Any use of GenAI with data defined as other than public requires pre-approval and authorization from the Office of Information Security – Chief Information Security Officer (CISO).

- **Copyright and Intellectual Property**: All students, faculty, and staff must adhere to institutional standards of conduct. Many public-domain GenAI tools do not specify the data sources used to train the technology. As a result, there is a risk that GenAI tools generate copyrighted responses without proper acknowledgment. It is important to review the output of an AI tool to avoid plagiarism. In addition, other sources of information should be used to cross-check the accuracy

[1] For more information on what Generative AI is and how it works, see https://www.techtarget.com/searchenterpriseai/definition/generative-AI

and provenance of any AI output. In addition, please be aware that your intellectual property, if uploaded to a GenAI application, may no longer be protected and private.

- **Accuracy and Appropriateness**: Data used by GenAI tools may be inaccurate, inappropriate, or contain biases. All results from GenAI tools should be reviewed and verified before publication or distribution.

- **Equity/Opportunity**: Some use of GenAI may affect whether or not specific individuals can participate or feel comfortable participating. In addition, the cost of certain AI applications can be prohibitive for some individuals. Any use of GenAI should consider the impact on the source and target audience.

- **Transparency**: Ensure transparency regarding your use of GenAI. When using GenAI, cite its use properly. Also, be sure participants are all aware and consent to its use.

  Note: *Before purchasing or using any GenAI tool, submit a Temple pre-approval request to verify product* ***security, accessibility, and integration requirements****. Submit a request at: https://tuportal.temple.edu/group/home/purchasing-pre-approval.*

Principles

The following data types must **never** be used in any GenAI Public Data product:

- Any data classified as "Confidential" and "Sensitive" per the Data Usage, Governance and Integrity Policy (https://secretary.temple.edu/sites/secretary/files/policies/04.71.10.pdf) and <https://tuportal6.temple.edu/group/its/data-classifications> data classification grid, such as:

  - Personally identifiable financial information (NPI)
  - Protected Health Information (PHI)
  - Personally Identifiable Information (PII), such as Social Security numbers, driver's license or federal/state ID numbers, account numbers, credit card numbers, etc.

- Any works, patents, or inventions covered under the "Ownership" section of the Inventions and Patents Policy. https://secretary.temple.edu/sites/secretary/files/policies/02.53.01.pdfhttps://secretary.temple.edu/sites/secretary/files/policies/02.53.01.pdf
  - Intellectual Property (IP) – without appropriate permission and acknowledgment

- AI Notetakers - All other third-party AI note-takers (such as Reader.AI or Otter.AI) and any other third-party proxy are **prohibited** in all Temple-owned Zoom sessions, Microsoft Teams meetings, and other teleconferencing and meeting spaces. Temple University has no way to verify the security and privacy of these third-party tools. Furthermore, Temple cannot control what data these tools collect and how that data is used. Finally, a key difference between Zoom AI Companion and other third-party tools is that only the host of the Zoom meeting will control Zoom AI Companion functionality in the meeting.

If you have any questions, contact Temple's Technical Support Center by clicking the Request Help tab on the Information Technology Services home page or by calling **215-204-8000**.