Interim Policy Prohibiting Entering
Confidential Information into Generative AI

I. Purpose

Generative Artificial Intelligence (AI) tools such as ChatGPT and Google Gemini have garnered tremendous public attention. Members of the WPI community may be unaware that information entered into a generative AI tool immediately becomes part of the generative AI's information database. As a result, any private or confidential information entered into a generative AI tool is at risk of becoming public. This Policy is being put in place on an interim basis in order to deal with immediate risks of unintended disclosure of Confidential Information (defined below) while a more comprehensive policy is collaboratively developed.

As part of our ongoing efforts to keep our policies up to date, we will be collaboratively reviewing WPI's Data Classification and Usage Policy this year, as it was last revised in 2019. We will aim to integrate language related to generative AI usage into that revised policy.

II. Scope

This Policy applies to all students, faculty, and staff at WPI.

III. Definitions

"Confidential Information" means, for the purpose of this Policy, confidential WPI institutional data, confidential WPI employee data, and WPI student data that is not publicly available and should not be released publicly, including but not limited to:

- Social security numbers
- Financial account information
- Passwords
- Driver's license numbers
- Health care information protected under HIPAA
- Human Resources and personnel information
- Student records protected by FERPA
- Gift and Donor Information

IV. Policy

Do not enter Confidential Information into generative AI tools (e.g. ChatGPT, Google Gemini, etc.). The only exception is WPI Microsoft Copilot, which is the only approved AI platform for the use of "Confidential Information."

V. Questions

If you have any questions or concerns, you should seek guidance from your manager, Department Head or WPI's Information Technology Services (its@wpi.edu) before entering information in a generative AI tool.

* * *

Policy Sponsor: Chief Information Officer; Chief Information Security Officer
Responsible Department: Information Technology
Effective Date of First Interim Policy (i.e., date of Presidential Approval): December 4, 2023
Effective Date of Second (Extended) Interim Policy (i.e., date of Presidential Approval through end of extended interim period): November 26, 2024 – May 31, 2025
Effective Date of Third (Extended) Interim Policy (i.e., date of Presidential Approval through end of extended interim period): September 25, 2025 - March 26, 2026