Generative AI tools offer many capabilities and efficiencies that can greatly enhance our work. When using these tools, members of the University community must consider issues related to information security, privacy, compliance, and academic integrity.

View guidance on using and procuring generative AI tools such as PhoenixAI, OpenAI’s ChatGPT, Microsoft Copilot, and Google’s Gemini.

GUIDELINES ON USING AND PROCURING GENERATIVE AI TOOLS

1. PROTECTION OF UNIVERSITY DATA

The use of confidential data with publicly available generative AI tools is prohibited without prior security and privacy review. This includes personally identifiable employee data, FERPA-covered student data, HIPAA-covered patient data, and may include research that is not yet publicly available. Some grantors, [including the National Institutes of Health](https://grants.nih.gov/grants/guide/notice-files/NOT-OD-23-149.html), have policies prohibiting the use of generative AI tools in analyzing or reviewing grant applications or proposals. Information shared with publicly available generative AI tools may expose sensitive information to unauthorized parties or violate data use agreements. (Please see [Policy 601](https://humanresources.uchicago.edu/fpg/policies/600/p601.shtml) or definitions of confidential data and its use for more information.)

2. RESPONSIBILITY FOR CONTENT ACCURACY AND OWNERSHIP

AI-generated content may be misleading or inaccurate. Generative AI technology may create citations to content that does not exist. Responses from generative AI tools may contain content and materials from other authors and may be copyrighted. It is the responsibility of the tool user to review the accuracy and ownership of any AI-generated content.

3. ACADEMIC INTEGRITY

For guidance on how generative AI tools intersect with academic honesty, it is recommended that instructors contact the [Chicago Center for Teaching and Learning](https://teaching.uchicago.edu/). (See [Academic Honesty & Plagiarism](https://studentmanual.uchicago.edu/academic-policies/academic-honesty-plagiarism/) in the Student Manual for University policy.)

4. PROCURING AND ACQUIRING GENERATIVE AI TOOLS

Generative AI systems, applications, and software products that process, analyze, or move [confidential data](https://humanresources.uchicago.edu/fpg/policies/600/p601.shtml) require a security review before they are acquired, even if the software is free. This review will help ensure the security and privacy of University data.

Please contact IT Services by submitting our [Generative AI Tool Review form](https://uchicago.service-now.com/it?id=its_sc_cat_item_request&sys_id=bf48443e1b0886505c56b912cd4bcbf2) before acquiring or using any tools, add-ons, or modules that include generative AI technology with University confidential data, even if they are free. For more information, see the [Policy on the Use of External Services](https://its.uchicago.edu/policy-use-external-services/) and the [Policy of Procurement and Engagement](https://intranet.uchicago.edu/tools-and-resources/financial-resources/i-want-to-find-purchasing-resources/policy-of-procurement-and-engagement-of-services).

CONTACTS

If you have questions about the guidelines, please contact:

* **Kevin Boyd**, Chief Information Officer, at [cio@uchicago.edu](mailto:cio@uchicago.edu)
* **Matt Morton**, Chief Information Security Officer, at [ciso@uchicago.edu](mailto:ciso@uchicago.edu)