Guidelines for Using ChatGPT and other Generative AI tools at Harvard

Dear Members of the Harvard Community,

We write today with initial guidelines on the use and procurement of generative artificial intelligence (AI) tools, such as OpenAI's ChatGPT and Google Bard. The University supports responsible experimentation with generative AI tools, but there are important considerations to keep in mind when using these tools, including information security and data privacy, compliance, copyright, and academic integrity.

Generative AI is a rapidly evolving technology, and the University will continue to monitor developments and incorporate feedback from the Harvard community to update our guidelines accordingly.

Initial guidelines for use of generative AI tools:

- **Protect confidential data:** You should not enter data **classified as confidential** (Level 2 and above), including non-public research data, into publicly-available generative AI tools, in accordance with the University's **Information Security Policy**. Information shared with generative AI tools using default settings is not private and could expose proprietary or sensitive information to unauthorized parties.
- **You are responsible for any content that you produce or publish that includes AI-generated material:** AI-generated content can be inaccurate, misleading, or entirely fabricated (sometimes called "hallucinations"), or may contain copyrighted material. Review your AI-generated content before publication.
- **Adhere to current policies on academic integrity:** Review your School's student and faculty handbooks and policies. We expect that Schools will be developing and updating their policies as we better understand the implications of using generative AI tools. In the meantime, faculty should be clear with students they're teaching and advising about their policies on permitted uses, if any, of generative AI in classes and on academic work. Students are also encouraged to ask their instructors for clarification about these policies as needed.
- **Be alert for AI-enabled phishing:** Generative AI has made it easier for malicious actors to create sophisticated scams at a far greater scale. Continue to **follow security best practices** and report suspicious messages to **phishing@harvard.edu**.
- **Connect with HUIT before procuring generative AI tools:** The University is working to ensure that tools procured on behalf of Harvard have the appropriate privacy and security protections and provide the best use of Harvard funds.
  - If you have procured or are considering procuring generative AI tools or have questions, contact HUIT at **ithelp@harvard.edu**.
  - Vendor generative AI tools must be **assessed for risk by Harvard's Information Security and Data Privacy office prior to use**.

It is important to note that these guidelines are not new University policy; rather, they leverage existing University policies. You can find more information about generative AI, including a survey to collect data on its potential use, **on the HUIT website**, which will be updated as new information becomes available.

Sincerely,

Alan M. Garber
Provost

Meredith Weenick
Executive Vice President

Klara Jelinkova
Vice President and University Chief Information Officer