Privacy considerations for **Generative AI on Campus**

What is GenAI? It is a type of artificial intelligence tool that appears to mimic human creativity to generate new images, text, audio or video in response to user prompts.

We're all aware of the fast proliferation of generative artificial intelligence ("GenAI") tools, and, as a campus, we are grappling with these tools' academic implications. Data privacy concerns aren't unique to GenAI tools, but these tools represent heightened threats to data transparency and accountability, as well as to individuals' intellectual work and data privacy rights.

- **Commercial GenAI tools are not regulated; we should assume that anything we share may be used to train datasets and, like all other forms of digital communication, could become publicly available.**
  resource: ChatGPT users shocked to learn their chats were in Google search results
- **GenAI companies don't own the content they use to train their models. They argue that their unpermitted use of copyrighted artist and authors' work is "transformative" and thus falls under a Fair Use copyright exemption.** Litigation is ongoing, as data collection continues. resource: DAIL – the Database of AI Litigation
- **There are currently no AI-detection tools that are sufficiently accurate; they all suffer from too many false positives and false negatives.** Further, AI-detection tools more frequently produce false positives for non-native English speakers.

Protect Privacy: Don't disclose personal information

Most Generative AI companies build their large datasets by scraping publicly available content that was shared on the internet. Some companies offer ways to opt-out of some data collection.
resource: How to Protect Your Privacy From ChatGPT & Other AI Chatbots (Mozilla)
resource: Privacy of Personal Data in the Generative AI Data Lifecycle (NYU JIPEL)
resource: **Ithaka's AI product tracker** (a comparison chart by the company behind JSTOR).

Be anonymous: When interacting with GenAI tools, don't use a personally identifiable email address, like your Bard account (unless you are an early tester of Google Gemini in the Bard Google domain).

Ensure Students' Data Privacy

What information are you sharing about yourself or your students?

Third party, online educational tools (those you choose to use for coursework that are not supported by Bard IT) may incorporate GenAI functionality. Use of these educational tools may disclose your students' personal information and academic work, which could be used to build data sets to train GenAI, and could become public. *Depend upon a course tool not supported by Bard IT? Request an IT data security review.*

Protect Confidential Data (yours and your students')

Confidential data is personally-identifiable student information that all college employees are legally required to protect (see FERPA). Sharing student data or work with unapproved tools could be a FERPA violation. Protect your students' scholarly work, and shield their thinking or personal opinions.
resource: **Understanding FERPA in the Context of Generative AI: Faculty Guide**
resource: **Privacy Considerations for AI Systems (Yale)**

Creative Work: Don't give away intellectual property

- Don't give away someone else's intellectual property or labor. When interacting with GenAI tools, consider whether you want your work to be used to train a startup company's models.
- This means that faculty shouldn't submit a student's work to outside tools (don't share another's intellectual work without consent and don't share other's personal information - as this could violate FERPA). Accordingly, consider asserting your ownership of your course work; communicate with students that you do not give permission for your work, or others' work that you share in your course, to be submitted to GenAI "course research assistants."