Use AI Safely at CMU

Generative Artificial Intelligence (GenAI) tools enable the quick creation of new content based on data analysis and inputs. As these tools evolve, we must be aware of the associated data privacy, security, ethical, and legal concerns and use them responsibly.

Guidance

CMU has partnered with the following AI services to ensure approved university contract terms are in place when these services are accessed through Web Login with your Andrew userID and password:

- ChatGPT Edu
- Google NotebookLM
- Google Gemini Web App
- Microsoft Copilot Chat
- Zoom AI Companion

They may be used (including Custom GPTs, Google Gems, and Microsoft Copilot Agents) with any CMU data except Controlled Unclassified Information (CUI). Always follow CMU's Data Classification Guidelines and any sponsor/regulatory/contractual requirements.

Checklist: Use AI Safely at CMU

Before using generative AI tools, follow these steps to keep your data secure and use AI responsibly:

- **Review the** Guidelines for Data Classification to ensure the security of university data and protect the privacy of our students and colleagues.
- **Report suspicious activity**, such as phishing or synthetic media (e.g., Deepfakes), to the Information Security Office.
- **Copyright guidance regarding authorship is still unclear.** Adding personal modifications to Generative AI output may increase the likelihood of copyright protection, but exercise caution. Please be aware that current legal rules state that auto-generated content does not get copyright protection.
- **Review AI outputs for accuracy.** A human-in-the-loop is required to catch hallucinations or errors.
- **Always use CMU-licensed and approved tools when logging in with your Andrew userID and password**. Institutional safeguards do not cover tools not approved by CMU and should be considered “use at your own risk.”
- Review the university’s Computing and Information Security policies.

Also, consider these steps for your role:

- **Faculty:** Add a syllabus statement explaining what AI use is permitted in your course. Follow the Eberly Center’s guidance on course design and responsible AI use.
- **Staff:** Review the data types you can safely input into generative AI tools.
- **Students:** Read CMU's Academic Integrity Policy, especially the "Unauthorized Assistance" section.
- **Researchers:** Consult your grant agency’s guidelines.

CMU Guidelines

Academic Integrity Policy
Computing Policy

Course Design and Teaching
Data Classification
Digital Copyright and DMCA
Information Security

Learn more

Meet AI
What can I use AI for?
How do I use AI?
Protected AI Tools You Can Use

Know the Difference—Public vs. Protected AI Tools

Public AI Tools

When you use a public or free AI account, such as a personal or free ChatGPT account, or don’t log in with your Andrew account:

- You risk losing control over how your data is stored, processed, and reused.
- Your data could be stored and used to further train the model.
- CMU data could even be sold to advertisers or used to train the AI model.

Remember, these tools should only be used for general exploration. Never use public AI tools with student data, confidential research, or sensitive administrative tasks.

Examples:

- Any AI tool that you create an account for yourself with a personal email (e.g., Claude, Chat GPT, Jules, etc.).
- Any AI tool that you log into with your Andrew account that does not bring you to a CMU Web Login page.

Protected AI Tools

When you access an AI tool through a protected environment, such as CMU's approved AI tools:

- You retain control over how your data is stored, processed, and reused.
- Your data remains private and secure.
- Your data will not be sold to advertisers or used to train AI models.

Examples:

Protected AI Tools You Can Use at CMU

Sharing in GenAI

General Sharing: Custom GPTs, Google Gems, or Microsoft Copilot Agents that include Private, Restricted, or Restricted-Specified data as defined in CMU's Data Classification Guidelines may only be shared with individuals who have the appropriate access rights, as determined by the CMU Data Stewards.

Research Data Sharing: If a Custom GPT, Google Gem, or Microsoft Copilot Agent contains research data subject to a Data Use Agreement (DUA), the terms of the DUA must be followed. DUAs may impose further restrictions beyond CMU’s data classification requirements. Such research data is typically classified as Restricted-Specified under CMU's Data Classification Guidelines.

Use ChatGPT Edu Agents

ChatGPT Agents can perform complex, multi-step tasks, not only by researching and reasoning, but by taking actions on your behalf. Think of Agents as virtual assistants that can work with your files, navigate websites, connect to external data sources, and even fill out forms on your behalf while remaining under your control.

Get Started

To create an Agent:

1. Click the plus sign (+) in the chat field and select Agent Mode. Note: Please refer to OpenAI's Usage Limits before exploring agent mode.
2. Enter a prompt outlining what you would like ChatGPT Edu to automate.

Note: Refer to CMU AI Tools Guidance for use and sharing restrictions.

Work with Agents

Check out these resources from OpenAI to continue learning about Agents.

- ChatGPT agent
- Introduction to ChatGPT Edu Agents
- ChatGPT Agent: Bridging Research and Action

- Use AI Safely at CMU

Best practices for data safety and reducing privacy risks

- Avoid typing passwords or private info directly in messages; use takeover mode for sensitive inputs.
- Enable only the connectors needed for the current task.
- Consider the data sensitivity of sites you log into via the agent.
- Avoid vague, open-ended prompts like “Check my email and handle everything.”
- Stop tasks immediately if something seems suspicious.
- Clear remote browser data after sensitive sessions.
- Regularly review and manage connector permissions in your settings.