

Tips for Students on Using AI Safely and Responsibly

- Ask if there are approved or recommended apps.
- Check on your course, institutional, or work policies.
- Be careful linking accounts. Create accounts not linked to other information.
- For paid accounts, investigate alternative payment methods.
- Be careful with using apps that bypass or break the rules of the LLMs.
- Check if information can be deleted.
- Check on how information is used.
- Check your privacy settings
- Do not give an AI personal or intimate information.
- Fact-check.
- Use only web versions of AI tools if concerned about data security.

Be careful what GenAI apps you use. At present, August 2024, the safest option for many purposes is Bing Copilot (sometimes called MS Copilot, though that also refers to other Microsoft products as well). This is a protected version of Bing Copilot that is available when you use your University ID to log into Copilot with your university account. (See [Appendix A](#).)

In some cases, you may be able to access the basic features of an AI tool without having to log in and may even be able to use an incognito window to further protect yourself.

With the current exception of Copilot, we do not recommend using your university email for AI logins. If you do, be sure that you do not use the same password. This is dangerous and against [University of Missouri policy](#).

If you do have to create an account and wish to preserve your privacy, you may use Google or other tools to create a separate email address not linked to any of your other accounts. (See [Appendix B](#) below.) If privacy or data security is a concern, do not login or link through Google, Apple, Facebook or other accounts. Login through an email address with a password or passcode instead. This prevents an AI from having access to those accounts. If you do link accounts, you may be able to change what data the AI can access through either the AI or the other account's privacy and security settings.

Many of the AI services allow you to delete sessions or conversations. In some cases, such as ChatGPT, you will see a trash icon when you mouse over a saved session. You may also want to check the settings of a given app to see if there is a feature there to turn saving sessions on and off. Finally, you can check the documentation, FAQs, etc. for an app to see if there is a feature available for deleting sessions and conversations. Likewise, you should check the documentation to see how saved information is used.

Because of the density and legalese in many privacy, terms of use, and other agreements, it can be difficult to determine exactly how your information may be used by an AI application. One technique that may be useful is to either copy the document into a chatbot (or if the AI has web access, give it the URL of the document) and ask it to summarize it, then ask follow-up questions. Note that some tools, such as ChatGPT have multiple documents that may apply. You may also be able to find articles online that critique the data usage of a given application but be careful to find reliable sources.

Most of the generative AI apps advise against providing them with personal or sensitive information. Many people ignore this. Never enter information relating to address, phone number, financial, medical information, etc. directly into an AI application. (A longer listing of kinds of information not to provide to an AI is listed in [Appendix C](#).) As Claude.AI writes: “The key is understanding what information an AI app truly needs and why, determining if it has responsible data practices, and not freely providing anything sensitive without that assurance first. If unsure, most private details should simply be left out.”

Fact-checking is necessary when working with these apps as they produce false statements (“hallucinations”) fairly often. See for instance the New York Times story, “Chatbots May ‘Hallucinate’ More Often Than Many Realize.” Some AI-specific things to look for:

- Try Googling quotes and follow any links to sources to see if they match up.
- If formal citations are listed, check to see if author, title, and date match up correctly.
- If using Gemini, you can now enable Google fact-checking by clicking the Google “G” icon at the bottom of its response. This will color code the text created by Gemini indicating it found corroborating content, conflicting content, or no matches.

Be aware of institutional policies governing the use of AI. For the University of Missouri System, please see: 200.010 Standard of Conduct, section C.1.c (the relevant passage

is quoted below in [Appendix D](#)). This gives your instructor control over what is and is not allowed with AI in the class. Check your syllabus and assignment instructions. If in doubt, ask your instructor.

Many AI tools have additional privacy settings. Some of these are summarized in [Appendix E](#). Also, you may find it easier to protect your privacy using the web version of these tools instead of phone, tablet, or laptop apps (see [Appendix F](#)).

See also our [Generative AI for Students](#) page.

Appendix A: About Bing Copilot

See also our [video tutorial on Copilot](#).

What is Bing Copilot with Data Protection?

Bing Copilot with Data Protection (formerly Bing Chat Enterprise) can access GPT (the same LLMs used by ChatGPT) and DALL-E for image generation. This version:

- de-identifies data (it is not associated with your account),
- sends and receives data in an encrypted manner,
- uses a private instance of OpenAI's tools (GPT and DALL-E) that OpenAI cannot access,
- data is not used for training the LLMs,
- when a session ends, the prompts (questions & instructions) and responses are deleted.

Like other Generative AI apps, while it is being reviewed, DoIT recommends that you do not enter any data that you would not wish to become public knowledge.

How do I access Bing Copilot?

You access Bing Copilot by logging into it with the same university credentials as you use for other systems, such as Canvas, Microsoft 365, or Outlook. It is available through:

- the Copilot button at the upper right corner of MS Edge,
- in Windows 11 through Windows Copilot in the taskbar,

- by logging into <https://copilot.microsoft.com/> in other browsers,
- through the Copilot extension for Apple Safari,
- through a Copilot app for iOS, iPadOS, Android, or Chromebook

Note that if you access Bing Copilot from a personal account, not a university account, the additional data protection is not enabled.

What can I do with it?

- Compose written content
- AI-assisted web search
- Summarize content from the web
- Use prompts in written or spoken form
- Upload images for it to summarize
- Generate images from written or spoken instructions

Tips:

- If you set it to **Creative** and **Precise** modes (Edge and web versions), Bing will use the more powerful GPT-4. In some mobile versions, you can explicitly switch on GPT-4. GPT-4 is much more powerful than the version used for the free version of Chat-GPT.
- When logging in through a browser other than Edge for the first time, you may need to change the SafeSearch setting in Bing's settings from **Strict** to **Moderate**.
- Because the session is deleted when it is closed, it is advisable to download or copy/paste your prompts and conversations to save offline.

Appendix B: Alternative Google Accounts

Open <https://google.com> in a browser window, incognito browser window, or new browser profile in a browser where you are not currently logged into Google, select **Sign In**, then choose **Create Account** and follow the instructions.

Note that Google does require you to use your real identity, so the security of this method is that it would keep a company from having access to your credit cards, other content or apps linked to Google, etc.

If you have a preferred browser and do not wish to use a different one for this purpose, try creating a new browser profile. Check your browser's help menu for how to setup and switch between different profiles, as this varies by browser.

You may also wish to experiment with different email providers, including those providing disposable email addresses, but at least some sites, including ChatGPT, exclude many of those domains, and continuing use may be difficult.

It is also possible to simply join your Google (or Apple, or other account) to an AI. This is quicker and easier than using an email username with a password or passcode. The downside is you are probably giving the AI access to at least some of your files and other information. This is more secure.

Appendix C: Types of Information Not to Share with a Chatbot According to ChatGPT-4

1. *Personal Identification Information:* Avoid sharing details like your full name, birth date, Social Security number, passport number, driver's license number, and other government-issued identification numbers.
2. *Financial Information:* This includes bank account numbers, credit card numbers, debit card PINs, and other financial details like your income, investment information, or debts.
3. *Contact Information:* Be cautious about sharing your personal phone number, home address, email address, or the contact information of friends and family.
4. *Health Information:* Medical records, health insurance ID numbers, information about your physical or mental health conditions, prescriptions, and any other sensitive health-related information.
5. *Work-Related Information:* Confidential information related to your job, such as work ID numbers, login credentials, proprietary data, or sensitive information about your employer or colleagues.
6. *Educational Records:* Personal educational records, transcripts, or any other confidential educational information.

7. *Passwords and Security Codes*: Never share passwords, security codes, or any other authentication data that could compromise your online security.
8. *Legal Matters*: Information about ongoing legal matters, court cases, or any legal disputes you might be involved in.
9. *Photos and Videos*: Be cautious about sharing personal photos or videos that could be used to identify you or your loved ones, especially if they include geolocation data.
10. *Biometric Data*: Information like fingerprints, facial recognition data, DNA information, or other biometric identifiers.
11. *Children's Information*: Avoid entering information about children, especially without proper consent or in violation of children's privacy laws (like COPPA in the United States).
12. *Sensitive Personal Beliefs*: Information about your religious beliefs, political opinions, sexual orientation, or other personal beliefs that could be used in a discriminatory or harmful way.
13. *Travel Plans*: Specific details about your travel plans, locations, and schedules, as these could be used for nefarious purposes.
14. *Internet History or Behavioral Data*: Details about your internet browsing history, purchasing behavior, or other online activities.

Appendix D: [200.010 Standard of Conduct, section C.1.c](#)

The term **unauthorized use of artificially generated content**, includes, but is not limited to (i) use of artificial intelligence tools or other tools that generate artificial content in taking quizzes, tests, examinations, or other assessments without permission from the instructor; (ii) submitting work for evaluation as one's own that was produced in material or substantial part through use of artificial intelligence tools or other tools that generate artificial content without permission from the instructor; (iii) using artificial intelligence tools or other tools that generate artificial content in a manner contrary to instructions from the instructor; or (iv) using artificial intelligence tools or other tools that generate artificial content in a manner that violates any other provision of these rules concerning academic dishonesty. Use of commonly available tools such as spelling or grammar checking software or features of software that propose anticipated words or phrases while text is being written will not be considered

unauthorized use of artificially generated content unless such use is contrary to instructions from the instructor.

Appendix E: Privacy Settings and Tips for Some Common Generative AI apps.

Many tools have settings you can enable or disable to enhance privacy or may have alternate modes of use.

ChatGPT

- You can use ChatGPT anonymously without logging in through the web. This is a limited version, at this time using ChatGPT-4o Mini.
- Free & Paid versions:
 - **General** settings allow you to **delete all chats**.
 - **Personalization** settings allow you to:
 - Set **Custom instructions** - while this can be helpful in getting consistent results, be careful what the instructions you create might reveal.
 - Turn off **Memory** - this will keep it from learning details about you. If you do choose to use this, you can use the **Manage** button to remove specific items or you can **Clear ChatGPT's Memory**
 - **Data Control** settings allow you to **Manage Shared Links** (removing them if desired) and you can also delete your account from here (there is an option to export data first).
 - The most important setting in this section is **Improve the model for everyone**. Toggle this off to prevent OpenAI using your data to train its models.
 - Be careful of links or connections you create in the **Builder profile** or **Connected apps** settings.
 - **Security** settings allow you to enable **multi-factor authentication** or **log out of all devices**.
 - There is a **Temporary Chat** feature available under the ChatGPT version menu at the top left of the main window. This prevents chats from being saved to history or used for training.

Perplexity.AI (<https://www.perplexity.ai/hub/faq/ai-profile>)

- You can use Perplexity anonymously without logging in through the web.
- Free and paid versions with login:

- There is an incognito mode for anonymous use. Click on your account name.
- Under settings, you can change your username and avatar (but not your email), disable **AI Data Retention** (for training data), sign out of all sessions, and **Delete account**.

Gemini (<https://gemini.google.com/>)

- Gemini has an unusual feature in its web version, it tracks your location. Your operating system should allow you to block this, but details will vary.
- Gemini allows you to delete old activity and to stop saving new activity. Google provides [extensive documentation](#) on how to do this on different devices and the web.

Appendix F: Web vs. App

There have been issues with privacy and security in the ChatGPT apps. This has included storing chats on Macs as clear text with no encryption. This would give a hacker access to chats on hacked machines. For best security and privacy, do not install ChatGPT apps. Also, if using desktop or mobile apps, be careful about giving access to files on your machine. This could compromise sensitive information.

In many cases, there is a tradeoff in functionality, for instance in conducting audio chats or the ability to import photos on the fly. Some of the apps are considerably more powerful in this regard to the web versions.

Last updated September 10, 2024