Protecting Information When Using AI Tools

Tuesday Mueller-Harder - 2023-08-25 - Comments (0) - Policy Frequently Asked Questions

AI tools such as ChatGPT, Bard, GitHub's Copilot, and others are widely available, and moving forward quickly in their abilities. These are often web services that can store, learn from, and possibly re-share the data you share with them. Here are some ways to make sure you are not exposing important or sensitive data to these services if you use them.

Do not share sensitive information with Open AI tools

Unless Brown has a contract for a specific service which protects our data, do not enter Level 2 or 3 data into publicly available or vendor-enabled AI tools. Without a contract, the owner of the AI tool usually claims ownership of all submitted data, allowing them to do whatever they wish with it. This risks exposing proprietary or sensitive information to unauthorized parties. Protecting Brown’s information is a shared responsibility for all of us in the Brown community.

Keep the same level of caution when interacting with AI tools for personal reasons. This is a rapidly evolving technology, and many of the associated risks and potential impacts are not yet understood.

Note, some AI tools are available to download and install on a computer you control yourself and any interactions with your data are more likely to happen only on that computer. In terms of protecting data, this is safer than using a web service with AI functions, because the data remains in your control.

Be mindful of new AI features appearing in your existing tools

As the AI market grows, more and more software applications and web services are adding AI features. This includes foundational services such as email, document editing, calendars, and video conferencing. Be sure to carefully review any access or permissions granted to any AI tool. Many of these AI features require deep and invasive permissions to read your information, and can result in the AI system having unexpectedly broad access to sensitive or personal material. If you need help reviewing any potential AI integrations, please reach out to help@brown.edu.

Take responsibility for your content

One of the most popular uses of AI tools is to help you quickly create new context-aware content, including communications, documentation, images, and software code. But ultimately you are responsible for any content you produce, share, or publish, even if you used an AI tool to help create it. AI-generated content can be inaccurate, misleading, or biased. What appears as facts can be completely invented, and you should make sure you

check any facts thoroughly before trusting its statements. AI tools can also produce content that is offensive, inappropriate, violate ethical standards, or contain copyrighted materials. Be mindful of AI's limitations, and extensively review any AI-generated content before sharing it with others or publishing it.

The National Institution of Standards and Technology's (NIST's) AI Risks and Trustworthiness framework is an additional resource that can help you determine which AI tools are safe to use.

Follow University policies

Use of AI tools is subject to the same policies as other information technology resources. Familiarize yourself and follow these guidelines at Brown:

- The Code of Conduct and Student Code of Conduct help ensure adherence to ethical, professional, and legal standards for our daily and long-term decision-making and actions.
- The Acceptable Use of Information Technology Policy helps ensure that confidentiality, integrity, and availability of Brown data is maintained.
- The Copyright Ownership and Use Policy defines the ownership of data and the importance of appropriate attribution.
- The Contract Review Policies and Process requires all contracts be reviewed by an authorized reviewing office before software is purchased or used, which helps ensure Brown data is properly protected. OIT should review the procurement of any information technology resources. This includes services and applications that interact with Brown data, as well as hardware, software, technology related services, and cloud solutions.

AI technology is evolving rapidly. However, Brown's current technology policies address the use of AI. Experts across Brown are tracking AI system developments, and adopting policies, standards, procedures, and guidelines to help support our community to leverage this evolving technology in a productive, secure, compliant, and ethically appropriate manner.

Related Content

- Generative AI as a Research Tool