**Announcing Campus-Wide Access to Microsoft Copilot with Data Protection**



We’re pleased to announce the Microsoft Copilot with Data Protection service, a new service endorsed by Lamar University through the Center of Teaching and Learning Enhancement and Information Technology.

Microsoft Copilot with Data Protection, a generative AI-powered platform designed and created specifically for organizations, is now available for Lamar University faculty, staff, and students.

Previously branded Bing Chat Enterprise (BCE), Copilot with Data Protection ensures that organizational data is protected against threats. In Copilot with Data Protection, user and organizational data is protected–chat data is not saved, and chat data will not be available in any capacity to Microsoft or other large language models to train their AI tools against. This layer of protection is what sets Copilot with Data Protection apart from the consumer Copilot.

In addition, Copilot with Data Protection cites its generated content with verifiable citations, is designed to assist organizations in researching industry insights and analyzing data, and can provide visual answers including graphs and charts.

While it is built on the same tools and data as ChatGPT, Copilot with Data Protection has access to current Internet data, while the free version (3.5) of ChatGPT only includes data through 2021.\*

\*Note that while this tool is available to you immediately, future policies governing its use and related data may be released soon.

**Getting Started**

Navigate to [copilot.microsoft.com](http://copilot.microsoft.com/) and log in using your LEA ID and password. When signed in, look for a message confirming “Your personal and company data are protected in this chat” above the chat input box and a green “protected” notice in the upper right corner to ensure you are using Copilot with Data Protection. You should also note the Lamar University logo and name in the top left corner if you are logged in correctly. Copilot with Data Protection is currently available to Edge (desktop and mobile) and Chrome (desktop), with support for other browsers coming soon. It is not currently supported on the Bing mobile app for iOS or Android.

A screenshot of a computer

Description automatically generated

Example of Copilot with Data Protection when logged in using LEA ID and password.

Tips for using Copilot with Data Protection

* **Be cautious.** Lamar University only allows information that can be publicly available to be entered into generative artificial intelligence tools, including Copilot, without appropriate approvals.
* **Log in.** Always ensure you are logged in with your LEA account when using to ensure data is protected.
* **Potential uses.** Content generation, course development assistance, brainstorming, data analysis, document summarization, learning new skills, writing code, and more. Faculty should visit [CTLE](https://www.lamar.edu/ctle) for ideas.
* **Judicious use.** When using Copilot with Data Protection, exercise care when entering information into the prompt. Copilot with Data Protection is being offered for use with Public Information only. Any other levels of data sensitivity should not be entered. As with other services, we do not recommend the inclusion of personal information about yourself in prompts. To ensure privacy is maintained, you may not enter personal information of any coworkers, students, or others. Failure to follow this guidance may result in violations of law (e.g., FERPA, HIPPA, etc.). Similarly, when using the service, you must ensure adherence to copyright and intellectual property protections. See more considerations for protecting privacy when using Generative AI tools below. Note that you must abide by all existing privacy, technology, data, and acceptable use policies already existing for Lamar University and the Texas State University System.

**Protecting Privacy in Copilot and other Generative AI Tools**

Generative AI, encompassing artificial intelligence models creating content in various forms, such as text, images, and audio, employs deep-learning algorithms and training data to produce new content approximating the training data. In light of its growing popularity and transformative nature, the following general guidance is provided for Lamar University, with a focus on data privacy. ***Please note that this advice is not legal in nature and is not intended to be exhaustive.***

**If you use generative AI in regular work**

* Explore options to purchase or license a business or enterprise version of the software. Enterprise software usually brings contractual protection and additional resources such as real-time support.
* Begin discussions with your colleagues about the privacy considerations listed in the next section.
* Consider where and how existing policies and best practices can be updated to better protect user privacy.
* Remember to validate the output of Generative AI, and if using Generative AI in a workflow, consider implementing formal fact-checking, editorial, and validation steps to your workflow.

**If you create or develop generative AI:**

* Provide transparency about how your Generative AI models are trained. Inform users what data might be collected about them when using generative AI and create accessible mechanisms for users to request data deletion or opt-out of certain data processing activities.
* Explore incorporating privacy enhancing technologies in your initial design stages to mitigate privacy risks and protect user data. Consider technologies that support data deidentification and anonymization, PII identification and data loss prevention, and always incorporate principles of data minimization.

If you would like assistance as you consider data minimization, data anonymization, or data deidentification in your AI, the Privacy Team can help. Contact privacy@illinois.edu.

**Supplementary Guidance**

The realm of Generative AI is not novel, and apprehensions about its application and potential repercussions have been deliberated and will continue deliberations over time. Despite the recent surge in popularity and widespread access to generative AI capabilities, it is imperative to acknowledge the existence of established policies, practices, as well as scholarly, historical, and theoretical frameworks that should be considered alongside contemporary discussions. University employees must be careful to adhere to all relevant laws, university policies, and contractual obligations.

Within the university context, specific privacy laws, such as the U.S. Privacy Act, state privacy laws like PIPA, and industry-specific regulations including FERPA, HIPAA, COPPA, as well as global laws like GDPR and PIPL, are pertinent considerations. Given the unprecedented proliferation of AI and generative AI capabilities, market dynamics are fostering intense competition to integrate AI into existing offerings. This competitive pressure may compromise ethical standards and integrity when hastily introducing new features and capabilities to the market. Do due diligence.

It is essential to acknowledge that training data may encompass information collected in violation of copyright and privacy laws, potentially tainting the model and any products utilizing it. The societal and business impacts of such violations may only become evident over an extended period. We will continue to monitor these concerns.

Efforts to identify and remove personally identifiable information (PII) from large language models are relatively untested, potentially complicating responses to data subject requests within regulated timeframes. Additionally, the inclusion of PII in large language models may enable generative AI to expose such information in the output. The use of input data as training data, coupled with the interactive and conversational nature of data collection, may lead users to inadvertently share more information than intended.

Users may lack the technical literacy to discern that Generative AI mimics human behavior and can be intentionally misled into believing they are interacting with a human. The prolonged and conversational interaction may cause users to lower their guard, inadvertently divulging personal information. The extent of personal information, user behavior, and analytics recorded, retained, or shared with third parties remains unclear.

As generative AI becomes more mainstream, it is likely to follow established channels for monetization, potentially utilizing personal data for targeted advertising. Clear policies may be formulated regarding the retention and deletion of user data collected during interactions with generative AI systems. When contemplating tools to use, it is crucial to assess whether individuals can request the deletion of personal data, in line with GDPR and most other privacy laws.

Depending on their application, generative AI models may qualify as automated decision-making, thereby incurring heightened privacy and consent obligations. Under the GDPR, individuals have the right not to be subject to decisions based solely on automated processing with legal or similarly significant effects. Privacy laws in certain states grant individuals the right to opt out of personal data processing for profiling purposes.

Given the extended and conversational nature of many chatbot-based generative AI solutions, special attention should be given to minimizing legal and privacy risks related to wiretapping. Risks may arise under federal and state wiretap laws, and configuring generative AI solutions appropriately, with input from University Counsel may be necessary to mitigate these risks.

Generative AI models may be susceptible to adversarial prompt engineering, where malicious actors manipulate input to generate harmful or misleading content. This manipulation can lead to the dissemination of false information, exposure of sensitive data, or inappropriate collection of private information. It is important to critically evaluate the output of all generative AI tools.

The implementation of generative AI should prioritize transparency for users and be complemented by training and educational programs. Educating users about how AI models function, the data they collect, and potential risks can empower individuals to make informed decisions and take privacy precautions when engaging with such technologies. Promoting AI literacy within the University community is pivotal for understanding the privacy implications of interacting with generative AI systems. Lamar University is offering training through the CTLE and other offices as they become available.

Generative AI systems possess the capability to generate content that may unintentionally or intentionally defame individuals or organizations. Implementing vigilant measures to prevent the generation of defamatory content, such as robust content moderation, human review and editing, and filtering mechanisms, is essential. Clear policies may be established to address and rectify instances of defamation arising from the use of generative AI systems, ensuring accountability and safeguarding the reputation of the University and our communities.

Generative AI systems also have the potential to generate false, misleading, or inaccurate content. Users should be aware that the output created by generative AI may not be accurate or true, as these models do not evaluate outputs for factual accuracy. Instead, they assess outputs based on similarities to the training data upon which they are built. All outputs of generative AI should be critically evaluated before use.

**Resources**

To learn more or get help with Copilot with Data Protection, contact the Technology Services Help Desk, the Center for Teaching and Learning Enhancement, or review the [Microsoft Copilot with Data Protection](https://blogs.bing.com/search/november-2023/our-vision-to-bring-microsoft-copilot-to-everyone-and-more) resources.

**Special note regarding privacy, security, or misuse of AI:**

If a faculty member fails to adhere to privacy, security, and AI guidelines before Lamar University establishes more formal AI policies, the potential response from the university may include the following:

Warning and Education: The university may issue a warning to the faculty member, emphasizing the importance of following the guidelines and providing additional education on the proper use of generative AI tools, especially concerning data protection and privacy considerations.

Review and Assessment: The university might conduct a review of the specific instance where guidelines were violated. This could involve assessing the nature and extent of the violation, as well as its potential impact on data privacy and other relevant policies.

Temporary Access Restriction: The university may temporarily restrict the faculty member's access to generative AI tools or related resources while the review is ongoing. This measure aims to prevent further violations and protect the university community.

Policy Development Involvement: The faculty member might be encouraged to actively participate in the development of formal policies related to the use of generative AI. This involvement could include providing feedback, attending workshops, or engaging in discussions to shape the university's approach to these technologies.

Collaboration with Privacy Team: If the violation involves privacy issues, the faculty member might be required to collaborate with the university's Privacy Team to address concerns, implement corrective measures, and ensure compliance with relevant privacy laws.

Professional Development Opportunities: The university may offer professional development opportunities, such as training sessions or workshops, to enhance the faculty member's understanding of ethical considerations, privacy, and responsible use of generative AI tools.

Escalation to Higher Authorities: If the violation is severe or persistent, the university may escalate the matter to higher authorities within the academic structure for further investigation and potential disciplinary action.

Policy Enforcement: Once formal policies are established, any subsequent violations may be subject to the university's official disciplinary processes, which could include loss of privileged access, warnings, probation, suspension, termination, or other appropriate measures that may include civil or criminal prosecution.