AUBURN UNIVERSITY
AT MONTGOMERY

ADVISORY GUIDANCE: USE OF GENERATIVE AI TOOLS

Background:
With the emergence and widespread availability of public generative AI tools (GPT-4, ChatGPT, AlphaCode, GitHub Copilot, Bard, DALL-E 2, to name a few), many members of our community are eager to explore their use in the university context (example uses could include student academic work, faculty research, admissions, employee recruitment, etc.). Although AI tools have the ability to enhance such efforts, they also have the ability to cause harm if used improperly. The following guidelines have been established jointly by the Auburn Office of Information Technology, Auburn University at Montgomery Information Technology Services, the Office of the General Counsel, and the Office of Audit, Compliance & Privacy to help you identify and mitigate risks associated with the use of AI tools:

Definitions:

1. **Public Generative AI:** Public generative AI refers to generative AI models that are openly accessible and available to the general public. These models are often hosted on platforms or cloud services, allowing anyone to use them for various creative purposes, such as generating art, text, music, or even realistic images.
2. **Private Generative AI:** Private generative AI models, on the other hand, are deployed in a controlled, private environment. These models are used within closed systems or organizations and are not openly accessible to the general public. The primary focus of private generative AI is to ensure data privacy and security while still benefiting from AI-generated content.

Current Auburn University at Montgomery Environment: AUM currently does not deploy a private generative AI tool for institutional use.

Guidelines:

1. **Prohibited:** Data defined as "operational data" or "confidential data" in the Data Classification Policy should never be shared with, submitted to, or used with a public generative AI tool in the absence of specific, legally binding data security protection agreements and procedures.
2. **Allowable:** "Public data" as defined in the Data Classification Policy may be used freely in public generative AI tools, subject to the following restrictions:
    a. Users should have no expectation of privacy in data they input into public generative AI tools, or in output produced by the tool. In most cases, the tool retains the right to use any data you input or any output the tool produces. Accordingly, these tools should not be used to generate output intended for non-public use.
    b. Any purchase or acquisition of an AI tool must comply with the Software Acquisition Policy Instructors reserve the right to further restrict use of AI tools by students to complete academic work, in order to meet educational objectives. Students should be given clear and unambiguous expectations for use of AI tools, as well as awareness of disciplinary consequences of misuse.

Rationale for the Guidelines:

AUBURN UNIVERSITY
AT MONTGOMERY

1. **Data Protection:** AUM currently does not have broad data protection agreements in place with any of the public generative AI tools, and therefore any data shared with these tools cannot be considered to be protected.
2. **Personal Liability:** Most public generative AI tools use "clickwrap" or "clickthrough" agreements to get users to accept policies and terms of service before using the tool. Individuals who accept clickthrough agreements without University approval may face personal liability for compliance with the terms and conditions.
3. **Privacy:** Public generative AI tools are not designed to protect the privacy of your data; therefore, it is highly risky to input any confidential, proprietary, or otherwise sensitive information (PII, health information, ID numbers, financial information, etc.) into these tools.
4. **Intellectual Property:** You may not own intellectual property rights to the output of a public generative AI tool, and it would be risky to use these tools to produce non-public or proprietary results. Terms of usage often include language that the tool retains the right to use any output for the tool's own purposes. Finally, depending on the dataset used by the tool, your results may include unauthorized derivative works of others' copyrighted material, and you may find yourself at risk if you publish such work as your own.
5. **Cybersecurity:** A public generative AI tool itself may serve as a vector for malware or other cybersecurity threats to your systems, and standard risk mitigation practices should always be observed by users when using these tools on institutional systems.
6. **Accuracy:** Output of a public generative AI tool can be based on an almost endless array of tools, datasets, learning algorithms, and user inputs. Therefore, these tools may not in all cases produce accurate (or fully accurate) results within the context of your particular task. Caution should be exercised when relying on generative AI output, and a good practice is to treat AI tools as sources of ideas, rather than facts.
7. **Bias:** Public generative AI tool output may unintentionally produce biased, discriminatory, offensive, or otherwise undesirable results, especially if used in the context of admissions, recruitment, or disciplinary decision making. Again, use of these tools should be carefully reviewed before relying on results.

Further Information:
For questions regarding the appropriate use of AI tools, please contact the Auburn University at Montgomery Information Technology Services, the Office of the General Counsel, or the Office of Audit, Compliance & Privacy.

Further reading on this topic: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov).