Privacy Guidance for use of Artificial Intelligence

Artificial intelligence (AI) is a set of technologies that are based primarily on machine learning and deep learning and are used for data analytics, predictions and forecasting, natural language processing, intelligent data retrieval, and more. Artificial Intelligence can also assist with making recommendations or decisions, and solving complex problems. AI that can produce new content and ideas, including conversations, stories, images, videos, and music is called Generative AI or GenAI.

For the purpose of this guidance, *Artificial Intelligence Technology* will be referred as "AI Tools".

Use of AI tools present significant benefits. These powerful tools can assist with our daily operations, such as automating processes, increasing productivity, providing advanced data analysis and forecasting.

But use of AI also comes with **privacy considerations and inherent risks**. AI Tools that are trained with personal data, can suggest information about individuals that is not based on the information submitted by the user of the tool, which increases the privacy risks and concerns, even when the original data provided to the AI tool was considered non-sensitive. For example, when a generative AI model is trained on a large dataset of personal photos, it could potentially be used to create realistic but unauthorized images of individuals, raising privacy concerns.

Staff and faculty must be vigilant about the data they enter into any AI Tools, and must be certain that the use of AI Tools will not, in any way, violate GW's privacy, data protection and security policies and requirements.

Before using an AI Tool that accesses personal information of individuals, users should carefully consider whether it is necessary to include this information and whether the desired outcome can be achieved without personal details. Maximum privacy and security controls must always be employed to protect personally identifiable information (PII). Accordingly, when PII will be entered into an AI Tool, the AI Tool should be set with privacy enhancing settings to ensure that the PII is not retained by the AI Model and also, when possible, the PII should be anonymized.

AI Tools used at GW must not use personal information of our community members for training their models.

The following guidance is intended to govern the administrative use of AI Tools across the university and in all operations.

▸ Reviews and Approvals

Any implementation of artificial intelligence is subject to applicable university policies and standards, such as the Procurement Contract Review and Approval Process when purchasing information technology that includes AI capabilities.

When necessary to leverage the use of **AI Tools** that will process PII, the AI Tool **must be reviewed and approved**, by the GW Privacy Office and the Office of General Counsel. Before considering the use of an AI tool that would require entering personally identifiable information, make sure to obtain an Authorization to Operate (ATO) by GW Information Security.

The use of un-approved AI Tools for university operations and purposes will be considered a violation of university policies

related to privacy and data protection.

A list of AI tools approved for use within the GW community can be found on this page: Artificial Intelligence (AI) Evaluation & Status. Additionally, you can also Explore tools and resources with AI capabilities, available at GW to enhance teaching, learning, research, and administrative tasks.

Privacy Requirements

Use of AI must comply with the following requirements, under University Privacy Policies:

Transparency: AI systems intended to directly interact with individuals should be designed to inform users that they are interacting with an AI system, unless this is obvious to the individual from the context. *A chatbot, for example, should be designed to notify users that it is a chatbot. Another example is providing notice to individuals before enabling ZoomAI Companion and/or WebEx Assistant.*

Data Minimization: If the use of AI involves access to personal data, the principle of data minimization should be applied rigorously. With respect to Generative AI Tools, it is recommended that they operate in a "walled garden" regime, having limited access to university data and limited ability to sharing university data. **Only the minimum amount of personal information required should be used to achieve an objective.** Be especially careful with sensitive data when using AI tools and consider whether the data you are using will compromise regulatory, contractual, or legal obligations. For example, in Social Media, *when analyzing user behavior for targeted advertising, an AI system could use anonymized demographic data and aggregated interaction patterns rather than individual user profiles. Another example would be when, in research, an AI Tool is analyzing patient data to verify diagnosis, it should only use anonymized medical records, focusing on relevant health indicators instead of storing full patient histories.*

Data Security: AI tools may not be encrypted and present a variety of data security risks. Only AI Tools that received an Authorization to Operate (ATO) from GW Information Security may be used for university purposes and with university data.

Configure approved AI Tools for Privacy: AI Tools often offer **privacy-enhancing options** that users should enable when the use of AI involves entering personal information of GW community members. *For example, disabling the "automatic start feature" of ZoomAI Companion, to allow time for providing notice to meeting attendees and obtain their consent for the use of this AI Tool.* Consult with GWIT to learn more about privacy enhancing features of university approved AI Technologies.

Generative AI Tools should not be used alone (without human intervention) in any decision making processes, when the outcomes (decisions) impact our community members. That is because AI Tools can inadvertently learn and perpetuate unconscious or conscious biases present in the training data, which can lead to discriminatory outcomes, affecting privacy and fairness. *For example, Amazon famously built its own AI hiring screening tool only to discover that it was biased against female hires.*

Any potential use of AI Tools for surveillance and monitoring purposes requires extensive reviews and approval at the highest level. Contact the Privacy Office for further guidance.

Related Policies and Guidance

GW Privacy of Personal Information Policy

Contract Review and Approval Process

Data Sharing - Privacy Requirements

Privacy Considerations when using Virtual Meeting and Collaboration platforms

Cybersecurity Risk Assessments

GW Privacy Office

Email the Privacy Office

Report a Data Incident

Data Subject Requests