



Generative Artificial Intelligence Administrative Use Guidelines

Administrative policy approved May 13, 2024. Effective immediately.

Revision history: None; new guidelines.

Related policies: Information Security Policy; Data Classification and Handling Policy; Computer and Network Use Policy; Student Records Policy – FERPA; Policy to Prevent Discrimination, Harassment, and Retaliation; Website & Digital Accessibility Policy.

Scheduled Review Date: January 2025 (President and Dean’s Office, Information Technology, and General Counsel’s Office)

Table of Contents

- A. Background and Scope..... 2
- B. Capabilities..... 2
- C. Confidentiality, Privacy, and Data Security Implications..... 3
- D. Prohibited Uses 4
- E. Output Ownership..... 4
- F. Output Accuracy..... 5
- G. Output Bias 5
- H. Digital Accessibility and Inclusivity..... 6
- I. Procuring GenAI Tools..... 6
- J. Incident Reporting and Phishing Attempts..... 6
- K. Violations 6
- L. Disclaimer..... 6
- M. Policy Revisions 6

A. Background and Scope

A new wave of generative AI tools and services, such as ChatGPT, Google Gemini, Microsoft Copilot, Co-Counsel, DALL-E, Midjourney, Synthesia, Jasper, and Zoom AI (GenAI Tools), is changing how many institutions, including Southwestern Law School, conduct business. For these guidelines, GenAI Tools are defined as any third-party or publicly available software that employs machine learning, neural networks, or other forms of advanced artificial intelligence to autonomously generate content, perform tasks, or provide recommendations, adapting and learning from interactions without direct human input.

Tools like Word Editor, Word SpellCheck, and Grammarly are not considered GenAI Tools for purposes of these guidelines.

GenAI Tools create content in various forms, including text, images, and audio across many formats and media. These technologies can help streamline processes, activities, and tasks. But users must understand the risks of using GenAI Tools, including information and data security and privacy, accuracy, trademark and copyright violations, and bias.

This guidance is designed for Southwestern staff and other employees with administrative responsibilities when using GenAI Tools. The guidance applies to using any third-party or publicly available GenAI Tools that mimic human intelligence to generate answers, work product, or perform certain tasks. These guidelines do not address the acceptable use of GenAI Tools for faculty regarding teaching, research, or scholarship.

B. Capabilities

GenAI Tools can boost productivity, simplify labor-intensive tasks, and provide suggestions and information. Staff are encouraged to responsibly experiment with and harness the capabilities of GenAI Tools and incorporate them into their day-to-day workflows.

GenAI Tools can help with the following:

- Administrative assistance (e.g., drafting communications like memos, notes, emails, letters, slide decks, and social media posts);
- Event planning (e.g., creating event descriptions, schedules, and promotional material);
- Research assistance (e.g., potential alternative for Google);
- Job descriptions and postings (e.g., suggesting language for position overviews, key responsibilities, and qualifications);
- Policy drafting and review;
- Data analysis (in line with the prohibitions in Sections C and D);
- Workflow automation;
- Training and onboarding (e.g., developing training materials and FAQs);
- Developing possible interview questions;

- Website and communications content (e.g., drafting content for institutional information);
- Editing assistance (e.g., editing text for tone, clarity, and grammar);
- Creating or editing images;
- Generating narration or background music for presentations; and
- Brainstorming ideas related to projects.

GenAI Tools serve many purposes but are not meant to solve all problems, especially when human empathy and connection are required. GenAI Tools are useful but are not a substitute for emotional intelligence, human judgment and subjectivity, real-world experiences, and creativity.

Staff should discuss any GenAI Tools they propose to use for work purposes with their department heads to ensure that using these tools is appropriate for the work being completed. Department heads unfamiliar with the proposed tool should seek input from IT or another knowledgeable department head or dean.

Southwestern staff are responsible for all work generated using a GenAI Tool and should not use work generated by a GenAI Tool without carefully checking its accuracy, currency, and legality (e.g., avoiding copyright violation, defamation, etc.).

Southwestern staff must follow Southwestern policies when using GenAI Tools.

C. Confidentiality, Privacy, and Data Security Implications

Entering data into many GenAI Tools is like posting that data on a public website. GenAI Tools often collect and store user data as part of their learning process. Accordingly, data entered into a GenAI Tool becomes part of its training data, which it may then share with other users outside Southwestern. Users should avoid entering personal, confidential, or otherwise sensitive information into a GenAI Tool.

Currently, Southwestern does not have enterprise contracts or agreements with any GenAI Tool provider. No GenAI Tool meets Southwestern's security, privacy, and compliance standards for handling anything besides public data. Therefore, Southwestern staff may enter institutional data into GenAI Tools only when the information is classified as public under Southwestern's *Data Classification and Handling Policy*.

Users should not enter any information into a GenAI Tool that is restricted by law (e.g., FERPA, HIPAA, copyright, etc.), contract, or Southwestern policy (e.g., personal information as defined in Southwestern's *Information Security Policy* and *Data Classification and Handling Policy*) or that is otherwise confidential, proprietary, or protected. Similarly, users should not enter sensitive information (e.g., information related to employees and their performance) and information classified as restricted or internal under Southwestern's *Data Classification and Handling Policy* into a GenAI Tool.

Questions about Southwestern's data standards and security should be directed to the Chief Information Officer by emailing ithelp@swlaw.edu.

D. Prohibited Uses

In addition to the prohibitions in Section C, Southwestern staff may not use GenAI Tools for the following purposes or purposes similar to those listed below:

- to generate content that facilitates sexual harassment, threats, stalking, hostile environments, illegal discrimination, or otherwise violates Southwestern's *Policy to Prevent Discrimination, Harassment, and Retaliation*;
- to upload data that could be used to help create or carry out malware, spam, and phishing campaigns or other cyber scams;
- to intentionally damage, disrupt, or expose Southwestern data to unauthorized access or harm;
- to hack or gain unauthorized access to a school network, security system, or other official system;
- to alter official records or fabricate data;
- to generate content that helps others break federal, state, or local laws; Southwestern policies; or agreements or contracts;
- to infringe copyrights or other intellectual property rights;
- to purposefully produce inaccurate or misleading information, including but not limited to deepfakes (i.e., photos or video or audio intended to convincingly mimic a person's voice or physical appearance without their consent), including ones that impersonate Southwestern staff, faculty, students, trustees, or public figures (other than for demonstration purposes in an educational setting).
- to create reports, spreadsheets, or other documents that include non-publicly available personal or student data (e.g., SSNs, FERPA-protected data and images; medical records, financial information, accommodation information, driver's license numbers, employee discipline);
- to select which job or admissions applicants will be selected for an interview or extended an offer; or
- to determine disciplinary action.

E. Output Ownership

GenAI Tools often draw upon the work of others, particularly trademarked or copyrighted work, to create content. At this point, it is unclear who owns outputs generated by these technologies. Until the courts resolve that issue, staff should avoid using GenAI Tools for projects when Southwestern must, for business purposes, own the final work product (e.g., official reports and publications). As with misinformation and bias, which are discussed below, users must carefully review and edit output from GenAI Tools to avoid plagiarism and misattribution.

Users must also analyze whether, for a particular project, they should acknowledge or disclose the use of GenAI Tools in their final work product.

A sample acknowledgment for text might read as follows: "The author generated this text in part with GPT-3, OpenAI's large-scale language-generation model [or insert other GenAI Tool used]. After generating draft language, the author reviewed and checked

factual information, edited and revised the language to their satisfaction, and takes ultimate responsibility for the content of this document.”

A sample acknowledgment for images might read as follows: “Foreground model created by Midjourney and sketched by the author.”

Users typically do not need to disclose the use of GenAI Tools for brainstorming, editing initial drafts, or minor tasks. A guideline to follow is whether a reasonable person would expect to know that you used a GenAI Tool to create your work product.

Staff should use additional care and sensitivity when using GenAI Tools to assist in creating public-facing documents, such as press releases, media releases, advertisements, webpages, social media posts, and similar material.

Staff should consult the General Counsel’s Office if they have concerns about content created with a GenAI Tool before publishing or distributing it.

In addition, to safeguard Southwestern’s reputation, all public communications and external publications using content generated to a significant degree by a GenAI Tool should be reviewed and approved by the Chief Communication & Marketing Officer to ensure consistency, accuracy, and alignment with institutional mission and core values.

F. Output Accuracy

Many GenAI Tools are large language models that predict what a human might say next in a given context. As such, GenAI tools may generate results that seem realistic but are inaccurate, misleading, or fabricated (“hallucinations”). GenAI Tools also have the potential to generate content that may defame individuals or organizations. Do not simply copy and paste GenAI Tools's output, especially for public-facing content. Do not trust any output generated from GenAI Tools; always review the information for accuracy and edit or revise as needed.

G. Output Bias

Many GenAI Tools are trained on datasets that are incomplete or include biased data. In addition, implicit and systemic biases can be purposefully or inadvertently built into GenAI Tools and their output. These biases are inconsistent with Southwestern’s mission and core values. Therefore, using outputs in a way that amplifies these biases can be contrary to Southwestern’s mission and core values.

To help reduce bias in final products, users should:

- Read the terms of service and other disclaimers associated with the GenAI Tool;
- Be aware of the origins of datasets used by the GenAI Tool;
- Consider how to reduce biased output through effective prompt engineering;
- Carefully review all output for bias.

H. Digital Accessibility and Inclusivity

When using GenAI Tools, users should prioritize creating outputs that are universally accessible and inclusive and conform to Southwestern's *Website & Digital Accessibility Policy*.

I. Procuring GenAI Tools

If you have procured or are considering procuring GenAI Tools or have questions, contact the Information Technology department at ithelp@swlaw.edu. Southwestern's Information Technology department must assess vendor GenAI Tools before use. No one may integrate any GenAI Tool with internal Southwestern software without first receiving permission from the Chief Information Officer.

J. Incident Reporting and Phishing Attempts

Any member of the Southwestern community who learns of a potential breach of data protection or confidentiality, including through the use of a GenAI Tool, must report the incident to the Information Technology department at ithelp@swlaw.edu.

If a member of the Southwestern community is concerned that someone has violated these guidelines, report the behavior to the individual's department head or Human Resources.

In addition, GenAI Tools have made it easier for malicious actors to create sophisticated phishing emails and deepfakes at a far greater scale. Report suspicious messages to ithelp@swlaw.edu.

K. Violations

Violating Section C or D of these guidelines may result in disciplinary action, up to and including termination, and could result in legal action. Failing to adhere to other guidelines may result in additional training, verbal or written counseling or reprimands, performance improvement plans, or similar actions designed to help the staff member comply with these guidelines.

L. Disclaimer

Nothing in this policy is designed or intended to interfere with, restrain, or prevent employee communications regarding wages, hours, or other terms and conditions of employment or any other rights protected by the National Labor Relations Act.

M. Policy Revisions

Southwestern expressly reserves the right to change or modify any aspect of this policy at any time, with or without notice.