DC COURTS AI INTERNAL USE POLICY

Purpose: This policy is intended to guide the cautious use of rapidly developing artificial intelligence (AI) technology.

Coverage: This policy governs the use of AI by all DC Courts' judicial officers, employees, contractors, and volunteers for court business and when using court information. The policy is not limited to a specific type of artificial intelligence, such as generative artificial intelligence. AI tools contracted for or developed for the DC Courts are exempt from this policy but may be subject to any subsequent policies and rules.

I. DEFINITIONS

Artificial Intelligence or AI – refers to technology that enables computers and programs to appear to learn, reason, or otherwise mimic human intelligence.

AI Tool – refers to an AI product, solution, or application, whether standalone or embedded, e.g. ChatGPT vs. Microsoft Co-Pilot or Westlaw AI Search.

Generative AI – refers to AI tools which can create new content through machine learning based on data input (which could include documents, images, audio, or video). Large Language Models (LLM's) are a type of Generative AI that have been trained on vast amounts of data, which the tool uses to mimic understanding of prompts and produce content including documents, images, audio or video.

Non-Sequestered System – This refers to virtually all free AI tools and a number of paid AI tools, where the confidentiality of data and prompts entered by the user may not be private to the user. Data entered by the user and the user's feedback could be used to train the system, among other potential purposes.

Sequestered System - A sequestered AI tool is one which the provider purports to protect the confidentiality of data and prompts entered by the user, e.g. the promised deletion of documents uploaded to the Westlaw and LexisNexis AI review functions. Generally, a sequestered system will require payment to access.

Public Court Information – refers to documents and information filed with, created by, or maintained by the Courts which the public can gain access to.

Confidential Court Information – refers to information that is made confidential by court order, court rule, regulation, or statute. It further refers to information which the user has access to because of the user's official position, which would not otherwise be available to the public. It includes court proprietary content, such as draft opinions, draft orders, internal court manuals, and work product prepared by court employees, contractors and volunteers.

Sensitive or Personally Identifying Information – refers to any information that when used alone or in combination with other data can identify or trace and individual, such as date and place of birth, mother's maiden name, social security, driver license,

financial account, medical, educational, employment, and court numbers, and any other content.

II. DECISION MAKING

Users may not delegate decision-making responsibilities to any AI tool. Generative AI tools are intended to support (or aid) decision making and are not a substitute for judicial, legal or other professional judgment or expertise.

III. COMPLIANCE WITH RULES GOVERNING THE USER

It is the responsibility of the user to be aware of and comply with all laws, rules, codes of professional conduct, and court policies, including ethics rules, which govern the work they intend AI to support. This includes the duty to review and confirm the accuracy of all output from any AI tool, including checking such output for bias, and to review and confirm that data provided to an AI tool is allowed under this policy before uploading it.

IV. USER RESPONSIBILITY AND INFORMED USE

Any use of AI is the responsibility of the user in all aspects, from entering data and instructions (prompts) to supporting or promoting AI-generated content. The user is responsible for reviewing and ensuring the accuracy and dependability of AI derived work product. To that end the user must take mandatory court-offered AI training as a baseline and is encouraged to seek further training. Further, the user should not use a tool without investigating and understanding the terms and conditions, technical capabilities, and limitations of the tool. Caution should be exercised, especially in ensuring the protection of confidential court information.

V. USE OF COURT TECHNOLOGY AND RESOURCES

Users should exercise caution in using any court issued technology to access AI tools which are not provided by the courts.

a. No court email address or user id should be used to register for access to a non-sequestered system.
b. No non-sequestered system may be locally installed on court-owned devices nor on personal devices used to access confidential court information.
c. A user may not use their passwords for court provided applications as a password used to access any AI tool not provided by the courts.
d. Additionally, in line with the DC Courts password security policy, a user should:
    i. Use a strong password that is at least eight characters long, including at least three of the following categories—upper and lower case letters, numerals, and special characters—as allowed by the AI tool provider.
    ii. Passwords may not include dictionary words, common names, portions of associated account names, consecutive character strings (e.g. abc, 123), simply keyboard patterns (e.g. qwerty, asdfg), generic passwords (e.g. a password consisting of a variation of the word “password,” like “P@ssw0rd1”;
    iii. Passwords should be changed at least every 90 days; and
    iv. If offered, a user must opt for two-factor authentication.

VI. CONFIDENTIALITY

No court information, whether public or confidential, should be entered into a non-sequestered system. No confidential information should be shared with an AI tool. No sensitive or personally identifiable information should be shared with an AI tool. Judges and judicial staff in particular should be cautious, especially in using non-sequestered systems, to avoid providing information that could disclose internal deliberations.

VII. DATA SECURITY

Data security is a primary concern in the use of AI tools. If a user suspects that an issue has arisen in their use of an AI tool, including, but not limited to, a security breach, such their password being compromised, or that information has been shared with an AI tool that should not be, the user shall immediately:

a. Notify their manager;
b. Report any known or potential security breach to the IT Security Branch;
c. Immediately change their password, if compromised;
d. Report any known disclosure of sensitive, personally identifiable of confidential court information to the General Counsel's Office; and
e. Follow any terms the AI tool provider offers to rectify the situation, e.g. a request for deletion of data.

VIII. **INTERNAL USE REPORTING**

Supervisors may set internal disclosure requirements for their teams regarding the use of AI tools in preparing court work product.

This policy was promulgated on [05-16-2025]. It is subject to continued review and amendment. The last amendment occurred on [05-16-2025]. Please see attachment A for a list of court approved and contracted AI tools and attachment B for a list of policies which affect court personnel use of AI.