

INTERIM POLICY ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE BY JUDICIAL OFFICERS AND COURT PERSONNEL

Section 1: Definitions

- A. “Administrative Records” includes notes, memoranda, correspondence, drafts, worksheets, and work product of Personnel of the Unified Judicial System, whether maintained in paper or electronic formats.
- B. “Artificial Intelligence” (“AI”) means the capability of computer systems or algorithms to imitate intelligent human behavior.¹
- C. “Case Records” are documents for any case filed with, accepted, and maintained by a court or custodian or any dockets, indices, and documents (such as orders, opinions, judgments, decrees, transcripts, and case exhibits) for any case created and maintained by a court or custodian. This definition applies equally to case records maintained in paper and electronic formats.
- D. “Leadership” means the Chief Justice of Pennsylvania, the President Judge of each appellate court and judicial district, and the Court Administrator of Pennsylvania, or their designees.
- E. “Personnel of the Unified Judicial System” (“Personnel”) includes (1) all state-level court employees including contractors of the Administrative Office of Pennsylvania Courts (“AOPC”), (2) all judicial officers of the Unified Judicial System as defined in 42 Pa.C.S. Section 102, including those granted senior status, and their staff, (3) all employees of boards, committees, and court-related panels established by the Supreme Court of Pennsylvania, and (4) all county-level court employees who are under the supervision and authority of the President Judge of a judicial district of Pennsylvania.
- F. “Generative Artificial Intelligence” (“GenAI”) means algorithms and/or computer processes that use artificial intelligence to generate text, audio, or images based on user prompts. These systems may be (and, presently, mostly are) trained on sets of data from the Internet or proprietary sources.
- G. “Non-Public Information” includes any and all information that is restricted by federal law, state law, policy, and other relevant legal authority. For examples, see Sections 9.0 and 10.0 of the *Case Records Public Access Policy of the Unified Judicial System of Pennsylvania*, and Section 3.00 of the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*. For further

¹ “Artificial intelligence.” Merriam-Webster.com Dictionary, Merriam-Webster, <https://www.merriam-webster.com/dictionary/artificial%20intelligence>. Accessed 10 Mar. 2025.

information on restrictions to public access of Unified Judicial System case records, please refer to the *Limits on Public Access to Unified Judicial System Case Records* posted at the Unified Judicial System Webpage.

- H. “Non-Secured AI System” means an AI system that does not protect and guarantee the confidentiality of data or documents entered into the system by users. This includes a system that retains user documents or data, and a system that may use user documents and data to train an AI system or may release user documents and data to third parties.
- I. “Secured AI System” means an AI system that protects the confidentiality and privilege of all data and documents entered in the system by users. Secured AI Systems do not retain any such data or documents entered into the system, do not transfer or sell such data or documents to third parties, and do not expose such data or documents to the public domain. A “Secured AI System” may include a vendor’s use of a subcontractor if all data and documents entered into the system remain subject to the requirements and limitations specified in this paragraph.
- J. “UJS Technology Resources” means any and all computer equipment, mobile devices, software, network systems, telecommunications equipment and systems, email and messaging systems, data storage, hardware, peripherals, and other electronic systems and devices owned, leased, provided, and/or used by the Unified Judicial System (“UJS”). For purposes of this Policy, this term includes a personal device used by Personnel for work related purposes.

Section 2: Statement of General Policy

- A. This Policy applies to Personnel using GenAI on UJS Technology Resources. The purpose of this Policy is to promote and ensure the safe and appropriate use of GenAI by Personnel.
- B. Leadership is responsible for ensuring Personnel of the Unified Judicial System who fall under their supervision and authority comply with this Policy.

Section 3: Authorization and Use of GenAI Tools

- A. Personnel are authorized to use GenAI for work only as set forth in this Policy.
- B. Personnel may only use or install GenAI tools approved by Leadership on UJS Technology Resources.
- C. Although use of a GenAI tool may be approved by Leadership, Personnel may be required to seek supervisory approval for the use of a GenAI tool or at a minimum disclose use of a GenAI tool in their work product.
- D. Personnel are permitted to use their work email or word-processing accounts to use approved GenAI tools.
- E. Personnel may only use GenAI as permitted by this Policy if the use does not violate other policies, rules, regulations or statutes. Permitted uses of GenAI by Personnel include, but are not limited to, the following:
 - i. to summarize documents;
 - ii. to conduct preliminary legal research, provided the GenAI tool used was trained on a comprehensive, up-to-date collection of reputable legal authorities;
 - iii. to draft initial versions of documents, such as communications, and memoranda;
 - iv. to edit and assess the readability of public documents; and
 - v. to provide interactive chatbots or similar services to the public and self-represented litigants.

Section 4: Responsibilities of Personnel

- A. When using GenAI, Personnel shall comply with all ethical and professional conduct rules and UJS policies, including but not limited to: the Code of Judicial Conduct, the Rules Governing Standards of Conduct of Magisterial District Judges, the Code of Conduct for the Employees of the Unified Judicial System, and the Rules of Professional Conduct.
- B. When using GenAI, Personnel shall comply with all applicable laws (*e.g.*, Personnel must ensure that copyrighted material is fairly used and properly attributed).
- C. Personnel must become proficient in the technical capabilities and limitations of GenAI tools before using them and must maintain competence to continue to use them.
- D. Personnel are responsible for the accuracy of their work and for compliance with this Policy.

COMMENTARY

Regarding Subsection A, Personnel shall observe high standards of conduct when they use GenAI so as to safeguard the judiciary's integrity and independence.

When using GenAI, Personnel must be cognizant that the systems may not consider nuances humans take into consideration. In addition, GenAI systems may be trained on biased material and generate biased content or harmful material. Furthermore, GenAI tools merely predict a probable outcome. Some of those predictions may be inaccurate because they have little or no basis in fact or reality (commonly referred to as "hallucinations").

Personnel must understand the limitations of GenAI tools and review GenAI output for accuracy, completeness, and potentially biased or inaccurate content. To repeat: humans must review GenAI output and Personnel are responsible for the accuracy of any GenAI information incorporated into their work.

Section 5: Permitted Use of GenAI

- A. Personnel may share with a secured AI system any case records, administrative records, or information provided that the shared information will be treated in a confidential and privileged manner. This means the secured AI system provider and its vendors will not use the records or information to train an AI system, share the records or information with unauthorized third parties, or expose the records or information to the public domain.
- B. Personnel shall not share any non-public information with non-secured AI systems.

COMMENTARY

Personnel are responsible for identifying non-public information. Personnel shall assume that case records, administrative records, and information will not be treated as confidential and privileged once entered into a non-secured AI system.

Any questions by Personnel regarding the use of GenAI should be raised through appropriate supervisory channels.

Section 6: Policy Implementation and Enforcement

Leadership in each court shall use due diligence to ensure compliance with this Policy, including thoroughly reviewing any contract with a vendor, as well as any end user licensing agreement during the procurement process.

COMMENTARY

For those contracts and end user licensing agreements entered into prior to the effective date of this Policy, Leadership shall review them to determine if Personnel are able to continue to use the services and products. In some judicial districts where non-judicial county personnel are responsible for technology contracts, Leadership must ensure that all GenAI tools comply with this Policy before authorizing their use. Areas for consideration should include whether the AI system vendor and any subcontractors retain any data, whether the AI system is a secured or non-secured system, the security of the system transmission pathways, whether the contract permits the vendor and any downstream subcontractors to view or use the content, and whether the content is exposed to the public domain.