Arizona Court of Appeals

Policy Number: HR – IT200	**Issued: April 29, 2024**
Subject/Title: Artificial Intelligence	**Effective: April 29, 2024**
Policy Section: Electronic Communications	**Revised:**
Policy Owner: Human Resources COA 1 and COA 2	

I. Overview

The use of certain artificial intelligence (AI) tools can provide benefits but also pose risks to court operations, litigants, and counsel. AI tools have the potential to enhance productivity by assisting with tasks such as drafting documents (other than drafting memorandum decisions and opinions), editing text, generating ideas, summarizing data, and software coding. However, AI tools also come with potential risks, including but not limited to, plagiarism, copyright infringements, inaccuracies, disclosure of confidential information, and bias.

II. Policy

Court personnel are expected to adhere to the following best practices when using AI tools:

1. **Purpose:** The Court of Appeals aims to integrate AI tools when beneficial and appropriate, but this policy does not allow the use of AI tools to abdicate the judicial decision-making role. This policy outlines the appropriate and permissible use of all AI tools.

2. **Scope:** This policy applies to all judges, staff, externs, and contractors involved in the court's operations. Court personnel includes all four categories.

3. **Court list of AI tools:** The court will maintain a list of AI tools, which will fall into three categories: (1) approved for all purposes, (2) approved for non-confidential information only, and (3) requires approval. The most current list is maintained at _____.

4. **Confidential data, court proprietary material, and Criminal Justice Information Services (CJIS) data.** For purposes of this policy:

    a. Confidential data includes, but is not limited to, information protected from public disclosure by law, court rule, or court order. Examples include:

        i. Confidential and personal financial records. Ariz. Sup. Ct. Rule 123(c)(3).

        ii. Mental health case records. Ariz. Sup. Ct. Rule 123(d)(6).

        iii. Juror records. Ariz. Sup. Ct. Rule 123(e)(10).

iv. Family court records that are closed or deemed confidential. Ariz. R. Fam. Law P. 13(e).

v. Juvenile court records that are closed or deemed confidential. Ariz. R. Juv. Ct. 215(a)(1)(C), 215(a)(2)(b), 313(a), and 403(a).

vi. Sensitive data as outlined in Ariz. R. Civ. P. 5(e) and Ariz. R. Fam. Law P. 43.1(f).

vii. Information filed under seal or subject to a protective order.

b. Court propriety data includes internal court data not meant for release to the public such as Notes, drafts, work product, and memoranda prepared by judges, attorneys, and law clerks employed by the court or court personnel at a judge's direction. Ariz. Sup. Ct. Rule 123(d)(4), (e)(9). It also includes internal court manuals.

c. CJIS data includes private or sensitive data gathered from local, state, or federal law enforcement agencies, including biometric data, such as fingerprints, and identity, person, organization, property, and case/incident history. It also includes criminal background information, copies of private documents, or anything else that could be classified as sensitive. It also includes CJIS-provided data necessary for civil agencies to perform their mission, including data used to make hiring decisions.

5. **Use of listed AI tools:**

a. Court personnel may use "approved for all purposes" AI tools in accordance with this Arizona Court of Appeals Artificial Intelligence Policy.

b. If an employee is preparing work or completing a task for a judicial officer, the court employee must get approval from the judicial officer before using an AI tool that generates content to complete the work or task.

c. Court personnel may use any "approved for non-confidential information only" AI tool except when working with confidential data, court proprietary data, or CJIS data. Court personnel may not use "approved for non-confidential information only" AI tool when working with confidential data, court proprietary data, or CJIS data.

d. Court personnel may not use any "needs approval" AI tools unless first having approval from the information technology office after consultation with the Chief Judge and Chair of the Artificial Intelligence Committee. Court staff, externs, and contractors also must have permission from their direct supervisor.

6. **Use of unlisted AI tools:** AI tools not included on one of the three lists are subject to this policy.

    a. Questions about unlisted AI tools should be directed to the court's information technology department.

    b. Because AI tools not included on one of the lists must meet the court's security and data protection standards, court personnel may not use any unlisted AI tools unless first having approval from the information technology office. Court staff, externs, and contractors also must have permission from their direct supervisor.

7. **Protection of confidential data, court proprietary data, and CJIS data:** Open-source AI tools are not secure. The input of confidential data, court proprietary material, and CJIS data into an open-source AI tool could result in the disclosure of that information to third parties.

    a. Court personnel who use AI tools must not upload or share any confidential data, court proprietary material, or CJIS data unless the AI tool keeps the information secure from third parties not employed by the court.

    b. Court personnel may input confidential data, court proprietary material, or CJIS data into AI tools on the approved list but not into any other AI tool without permission from the information technology office. Court staff, externs, and contractors also must have permission from their direct supervisor.

    c. Court personnel are expected to be familiar with applicable law and rules and use their best judgment to determine whether information may be subject to confidentiality before using any AI tool in connection with confidential data, court proprietary material, or CJIS data.

8. **Verification:** Court personnel are expected to recognize and understand the limitations of AI tools, avoid overreliance on such tools, carefully review output for errors, and remain vigilant to identify potentially erroneous, incomplete, hallucinated, biased, or otherwise problematic output. This obligation includes verifying case, rule, and statutory references with official sources. To that end, information generated by AI tools shall not:

    a. Be relied upon without scrutiny and verification with an official source.

    b. Be assumed to be truthful, credible, or accurate.

    c. Be relied upon as the sole source of reference.

9. **Misuse of AI tools:** Any misuse of AI tools, including but not limited to the violation of this policy, could result in disciplinary action as deemed appropriate.

10. **Amendments to this policy:** AI and the laws and regulations governing it are rapidly evolving. This policy may be amended from time to time to reflect changes in AI technologies, use, and governance.

ARTIFICIAL INTELLIGENCE POLICY ACKNOWLEDGEMENT

By signing this policy, I acknowledge that I have read and understand the requirements outlined in the Artificial Intelligence Policy. I agree to use AI tools in a manner consistent with the practices outlined in this policy.

Date: _____

Employee Name: _____

Job Title: _____

Department: _____

Employee Signature: _____

(Any online version of this acknowledgement must stipulate to the above content even if not worded identically.)