CCJ Council on Criminal Justice

Appendix J: General-Purpose AI Tools in Criminal Justice Settings

While the full sequential process in this framework (Phases 1–5) is designed for formal procurement of dedicated systems, the foundational questions in Phases 1 and 2 apply equally to general-purpose tools used in case-related work:

- **What problem is the tool being used to solve?** Staff using AI informally are making implicit judgments about fitness for purpose. Making these judgments explicit helps identify where AI assistance is appropriate and where it is not.
- **What are the risks?** General-purpose tools can fabricate plausible-sounding information (sometimes called "hallucination"), produce outputs that reflect biases in their training data, and may store or learn from data entered into them. These risks exist regardless of whether the tool was formally procured.
- **Is there meaningful human oversight?** An operator who pastes AI-generated text into a court filing without substantive review has effectively delegated a professional judgment to a machine. The oversight principles in this framework apply to that decision just as they apply to a risk assessment algorithm.

Recommended Action: Develop an Acceptable-Use Policy

Your agency should develop a policy governing staff use of general-purpose AI tools for case-related work. At a minimum, such a policy should address:

- **Permitted and prohibited uses.** Which categories of work may use general-purpose AI assistance (e.g., drafting routine correspondence, researching legal questions, analyzing data), and which may not (e.g., making recommendations about individual liberty, generating evidence summaries presented as original analysis, communicating with affected individuals)?
- **Data entry restrictions.** What types of information may be entered into general-purpose AI tools? Personally identifiable information, case-specific details, confidential informant data, sealed records, and other sensitive information generally should not be entered into external AI systems unless the agency has confirmed the provider's data handling practices through a formal review.

- **Review and attribution requirements.** All AI-generated content used in official work products should be substantively reviewed by the responsible professional. Such content should not be presented as original human work product without disclosure.
- **Documentation.** How should the use of general-purpose AI tools in case-related work be recorded? At a minimum, operators should be able to identify that AI was used, what purpose it was used for, what sort of review was conducted, and who performed the review.
- **Training.** Staff should receive training on the capabilities and limitations of general-purpose AI tools. Such instruction should include the tendency of these systems to generate confident but inaccurate outputs, the potential for bias, and the professional obligations that attend the use of AI assistance.

If your agency has already deployed purpose-built AI systems through formal procurement, you should also consider whether staff are supplementing those systems with general-purpose tools in ways that fall outside existing governance structures.