April 2024

from the **AI Rapid Response Team** *at the National Center for State Courts*

AI and the Courts:
Developing an Internal AI Use Policy

It is important for courts to develop an internal AI policy to ensure the responsible and ethical use of AI while enabling the organization to learn about and benefit from AI technologies and to minimize the risks.

Establish an AI Governance Working Group

Establish a working group to oversee the development and management of AI technologies and policies, ensuring consistency with the court's mission and values. The group should consist of representatives from all relevant stakeholders, including court leadership, business process, legal, and technology.

Assess the Court's Needs

Assess the current processes, identifying the court's goals and needs and determining whether the AI technology furthers them. When drafting an AI use policy, be sure to think broadly about a wide range of use cases. Identify the use cases that could benefit from AI tools, such as automating repetitive functions, data analysis, summarizing, drafting, or other tasks.

Assess the Risks

Assess the risks associated with implementing an AI tool, in areas such as hallucinations, data security, and staff concerns about job replacement. When drafting an AI use policy, think broadly about potential and perceived risks and address ways to mitigate them. Ensure that any new technology complies with any existing technology or security policies and technology infrastructure standards.

Understand the Technology and Contract Terms and Develop Procurement Requirements

Before implementing or purchasing any AI technology, understand what generative AI and other AI technologies are, how the technology will be used, the vendor's terms of use, and then develop applicable procurement requirements.

Considerations in Developing a Policy

When developing an AI use policy, consider including:

- the policy's purpose and scope: to whom it applies, to what technologies it applies, how it can be used, such as requiring the use of secure and encrypted networks when accessing or transmitting data through AI tools, and requirements about the use of court data for training AI tools;
- acceptable uses of AI that are responsible and ethical and comply with all applicable laws, regulations, and policies (*See Kentucky's and Utah's policies*);
- prohibited uses of AI that would jeopardize the court's network or potentially disclose confidential information; staff should not access, collect, use, or disclose personal or sensitive information beyond what is necessary for authorized business purposes;
- what data protection laws, regulations, or policies apply to the use of personally identifiable information and the data privacy and security measures that should be implemented or that employees should follow to protect the court's data;
- how to ensure that AI-generated content is not biased and does not reflect discrimination based upon race, ethnicity, gender, age, or other protected class;
- when to update and patch AI tools to protect against vulnerabilities and security risks, if not already covered in another security policy;
- mechanisms to monitor whether the policy is being followed, and plans for what to do if the policy is violated (security and HR).

Implement, Review, and Update the Policy

After adoption, communicate the policy to staff. Educate staff about the policy and how to responsibly and ethically use the AI tools. Schedule regular reviews of the policy and update it as necessary.