MD AI & A2J Community of Practice

Created by Leland Sampson

Last Updated: October 14, 2026

The following is a template that a legal service organization can use to create a generative artificial intelligence (AI) policy. The template is designed to be edited to suit your organization. Before drafting a policy, we recommend reading An Overview of Ethical Considerations for Attorney Use of Generative Artificial Intelligence Technologies.

Summary of Relevant Sections for Consideration

This summary section provides an overview of AI policy concerns and provides a framework for drafting your policy.

- **1. Purpose and Scope**: defines the organization's philosophy and policy on use of AI tools by attorney(s) and support staff. States the organization's commitment to ethical obligations and client-centric service.
    - Mandatory section
    - Relevant MARPCs
        - 19-305.1
        - 19-305.3

- **2. Definitions**: this template supplies a few generic definitions.
    - Mandatory section

- **3. Governance and Oversight**: defines the ultimate arbiter of data classification and AI use. This section designates the AI Governance Officer who is responsible for approving AI tools, overseeing their use, and ensuring compliance with this policy.
    - Mandatory section
    - Relevant MARPC: 19-301.3

- **4. Data classification and handling**: this section establishes a multi-tiered data classification system with escalating restrictions on how each data type can be used with AI tools.
    - Mandatory section
    - Relevant MARPC: 19-301.6

- **5. Authorized AI tools**: provides list of AI tools that have been reviewed by AI Governance Officer and authorized for use by staff.
    - Optional
    - Alternatives
        - Allow list where only these tools may be used

        - Block list where these tools may not be used

- **6. Authorized use of AI tools**: designates specific applications or workflows where AI use is allowed. Options include legal research, document drafting, administrative tasks, etc. Together with section 5, this section defines whether the organization will encourage or restrict the use of AI tools.
    - Optional section

- **7. Prohibited use of AI**: designates specific applications or workflows where AI use is not allowed.
    - Optional section

- **8. Verification and Responsibility**: AI tools are probabilistic, creative systems that mimic human outputs but do not possess human understanding. The purpose of this section is to impress upon staff using AI tools that constant vigilance is necessary. The human user will be held responsible for inaccurate or confabulated AI outputs or agent actions.
    - Optional section

- **9. Client communication and transparency**: statement of organization's policy on communications with clients.
    - Optional section
    - Relevant MARPC: 19-301.4

- **10. Training and competence**: establishes that AI tools may only be used by staff who have sufficient competency to use AI tools in compliance with this policy.
    - Mandatory section
    - Relevant MARPC: 19-301.1; 19-305.1

- **11. Security and confidentiality**: reminder of ongoing ethical and confidentiality concerns, stressing need to always be mindful of data classifications and authorized and prohibited uses.
    - Mandatory section
    - Relevant MARPC: 19-301.6

- **12. Policy violations**: establishes consequences for policy violations.
    - Mandatory section

- **13. Review and auditing**: defines how the AI Governance Officer will monitor use of AI tools by staff and build checks into workflows to catch any errors that may be produced by AI tools.
    - Mandatory section

[organization name]: Generative AI Policy

1. Purpose and scope

Encouraging: This policy establishes our approach to generative artificial intelligence (AI) technologies and their use by all staff. This policy is designed to harness the potential benefits of AI while remaining mindful of our ethical duties and commitment to the highest levels of client service.

Restrictive: This policy establishes our approach to generative artificial intelligence (AI) technologies and their use by all staff. While AI may evolve into an essential role within the organization's work, this nascent technology currently presents inherent risks and limitations. This policy is designed to allow for incremental testing of AI tools to identify best practices for mitigating risks and safeguarding confidential information. Any limited deployment of these tools should strictly adhere to the highest ethical standards.

2. Definitions

- AI Agents – AI systems that can perform tasks autonomously at the user's direction. AI agents can be designed with varying levels of human oversight, including multi-step tasks, interacting with external tools, applications, or data sources.
- AI Governance Officer – staff member responsible for implementing this policy.

3. Governance and oversight

This policy establishes the role of AI Governance Office within the organization and designates [insert name] to serve in that role. The AI Governance Officer has the following duties:

- Periodically review and revise the Generative AI Policy.
- Ensure all employees have read and acknowledged the policy.
- As new AI tools emerge, assess them for inclusion in the list of approved AI tools and provide employee training when new tools are approved.
- Periodically review workflows and work products to ensure adherence to the policy.

4. Data classification and handling

All organization and client data shall be classified according to the following tiered system. The restrictions on the use of data with AI tools increase with the sensitivity of the information.

- **Level 1: Public Data:** Information that is publicly available and poses no risk to the organization or its clients if disclosed.
    - **Content Examples:** Court opinions, published statutes and regulations, publicly filed documents, and organization marketing materials.

- **Level 2: Internal Data:** Information related to the organization's operations that is not intended for public disclosure but would not cause significant harm if inadvertently released.
    - **Content Examples:** Internal templates (without client information), non-confidential administrative schedules, and anonymized case statistics for internal analysis.
- **Level 3: Confidential Client Data:** Non-public information provided by or related to a client that is subject to the duty of confidentiality.
    - **Content Examples:** Client communications, draft legal documents, case notes, discovery materials, and any personally identifiable information (PII) of a client or opposing party.
- **Level 4: Highly Sensitive Client Data:** A subset of confidential client data that, if disclosed, could cause significant harm to the client, such as financial, proprietary, or privileged information.
    - **Content Examples:** Trade secrets, financial account information, medical records, and information subject to attorney-client privilege or a protective order.
- **Distinction between Level 3 and Level 4**: Documents or workflows that contain Level 3 data could have the confidential data removed and only the sanitized document may be used with AI. For example, when drafting a client communication, the client's PII should not be input into the AI tool. Level 4 data cannot be anonymized and may never be used with an AI tool.

5. Authorized AI tools

AI is the ability of technology to perform tasks commonly associated with intelligent beings. AI is a type of AI technology that can produce various types of content, including text as well as audio and visual material.

Deterministic software, where the output is always the same for a given input, is not covered by this policy.

Encouraging (block list): As long as the data classification protections have been respected, employees may generally use AI tools in their work. Remember that Level 3 and Level 4 data must be treated carefully. The following tools, however, may never be used:

- [this list may include specific applications or classes of applications. For example, the organization might not want to allow the use of image generators or AI Agents]

Restrictive (allow list): The following AI tools have been assessed by the AI Governance Officer and are authorized to be used where appropriate:

- [list specific tools or features of applications that may be used]

6. Authorized use of AI tools

[note: this section is optional. Depending on the type of policy you want to draft, you may want to only use either 6 or 7. If taking the restrictive approach, this section should be used. The bullet list below provides some inspirational ideas.]

AI tools may only be used for the following purposes:

- Initial research into a new or emerging area of law where rough summaries are helpful.
- To draft a paragraph or small section of a document where the author has an outline and clearly provides the desired parameters into the prompt. Remember that AI output should not be used verbatim and should only serve as a starting point for intensive editing.
- Assistance in parsing particularly dense or difficult to understand statutes.
- Assess the strengths and weaknesses of drafts in progress. Here, the AI tool should not suggest language options but provide objective analysis.

AI tools used for these tasks may only use Level 1 or Level 2 data. The use of AI with Level 3 or Level 4 data is prohibited. [The use of AI for drafting any client-facing document or court filing is prohibited.] If you are unsure about any aspects of the AI tool or your workflow, consult the AI Governance Officer.

7. Prohibited use of AI tools

[note: this section is optional. Depending on the type of policy you want to draft, you may want to only use either 6 or 7. If taking the encouraging approach, this section should be used]

This policy encourages the exploration and use of a wide range of AI tools to enhance productivity and client service. Level 1 data is not subject to any prohibitions. New AI tools may be provisionally used with Level 1 data for evaluation purposes before formal approval.

When using AI with Level 2 or 3 data, employees must use organization-approved, secure AI tools from the authorized list that have been vetted by the AI Governance Officer.

Level 4 data may not be used with any AI tool.

8. Verification and Responsibility

Staff must check and review all content generated by AI to ensure accuracy. AI tools can generate inaccurate or fictitious outputs. Even content a user sends to an AI tool may be altered in subsequent responses. All AI generated output must be verified by a qualified human. In particular, great care must be taken when reviewing AI-generated legal citations, quotations, and factual assertions. The human who uses the AI tool or creates the AI Agent is ultimately responsible for the output and actions of that tool.

9. Client communication and transparency

Encouraging: This policy does not require specific disclosures regarding the use of AI tools, as they are considered part of our standard practice. If an AI tool will be used in a unique or novel way in a client's case, written consent will be obtained from the client.

Restrictive: This policy requires full transparency regarding the use of AI in client matters. Engagement agreements must obtain informed consent from the client before using any AI tool on their behalf. The disclosure will explain the organization's reasons for using AI tools and confirm that all AI work product will be thoroughly reviewed.

10. Training and competence

All employees using AI tools must develop and maintain the requisite knowledge and skill to ethically and competently use the tools. The AI Governance Officer will provide initial AI training. This may include a mandatory course of study. The AI Governance Officer will monitor training needs as part of the policy review.

11. Security and confidentiality

Encouraging: As part of the vetting process, the AI Governance Officer will review the privacy and security policies of any AI tool approved for use. When exploring an AI tool, employees are reminded to use only Level 1 data and to review privacy and security settings. If an AI tool allows, prohibit the use of inputs for training data. Level 2 or Level 3 data may only be used with approved AI tools. Level 4 data may never be used with an AI tool.

Any suspected data breach or security incident involving an AI tool must be reported to the AI Governance Officer immediately.

Restrictive: As part of the vetting process, the AI Governance Officer will review the privacy and security policies of any AI tool approved for use. All access to approved AI tools will be through organization-managed accounts. AI tools may only be used with Level 1 or Level 2 data. The use of AI with Level 3 or Level 4 data is prohibited.

Any suspected data breach or security incident involving an AI tool must be reported to the AI Governance Officer immediately.

12. Policy violations

Adherence to this policy is paramount. Any violation of this policy may result in progressive disciplinary action. The following factors will be taken into account:

- Severity: the actual or potential harm to clients or the organization.
- Intent: whether the violation was accidental, negligent, reckless, or intentional.
- Frequency: Whether it is a first offense or a recurring pattern of non-compliance.
- Cooperation and mitigating circumstances

Disciplinary actions will be determined on a case-by-case basis and conducted by the AI Governance Officer. Disciplinary actions can include verbal or written warnings, suspension, or termination of employment.

13. Review and auditing

This policy shall be reviewed every six months by the AI Governance Officer to ensure it remains relevant and effective. The primary goal of the review is to adapt the policy to significant changes in AI technology and further develop organization workflows. The review should include checking changes to AI tool's security protocols, privacy policies, and terms of service.

The AI Governance Officer will periodically spot check reviewing work product and usage logs, to verify adherence to this policy. Ongoing discussions with all employees about their use of AI will ensure compliance, fostering a culture of responsible innovation, and shared accountability.