3-22-2026

Ethics Of Artificial Intelligence For Lawyers: Standalone Resource: Model Policy And Training Program For Responsible AI Use

Cliff McKinney
Quattlebaum, Grooms & Tull PLLC

Citation

McKinney, C. (2026). Ethics Of Artificial Intelligence For Lawyers: Standalone Resource: Model Policy And Training Program For Responsible AI Use. *Arkansas Law Notes*. https://doi.org/10.54119/aln.tkpd4178

ETHICS OF ARTIFICIAL INTELLIGENCE FOR LAWYERS: STANDALONE RESOURCE: MODEL POLICY AND TRAINING PROGRAM FOR RESPONSIBLE AI USE

Cliff McKinney*

Every significant technological change in law, including computers, email, and online research, has required practical tools to implement ethically. Artificial intelligence is no different. This final installment of the artificial intelligence ethics series offers a "starter kit" for responsible adoption by law firms: a Model Law Firm Policy on the Responsible Use of Artificial Intelligence and a Model Training Program for Legal Professionals.

The model policy provides firms with a framework for governance. This includes how to vet tools before approving them, how to maintain client confidentiality, how to verify all artificial intelligence outputs, and how to integrate disclosure obligations into engagement letters. The training program complements the policy by equipping lawyers and staff with the skills to use approved tools competently and securely. It outlines both baseline training for general use and advanced modules for higher-risk tools, emphasizing verification, confidentiality, and supervision. These resources are not one-size-fits-all solutions, but templates to be adapted by firms of different sizes and practice areas.

In full disclosure, I created both of these resources using artificial intelligence. I employed prompt engineering techniques to develop and refine the final products attached, which are not merely quickly generated by artificial intelligence. In fact, these took hours of refinement and adjustment to create. In addition to providing model forms, I also hoped to demonstrate the work

* J. Cliff McKinney is a Managing Member in the Little Rock, Arkansas office of Quattlebaum, Grooms & Tull PLLC.

product that can result from combining artificial intelligence tools with traditional legal and writing techniques.

With this installment, the *Ethics of Artificial Intelligence for Lawyers* series comes full circle. We have moved from the first sanction cases, to the ABA's initial guidance, to legislative and regulatory developments, and now to practical steps that firms can implement today. Artificial intelligence is here to stay, and lawyers must adapt. Adapting does not mean abandoning judgment to machines. Lawyers can smooth their transition to using artificial intelligence by creating policies and training that preserve professional responsibility in an artificial intelligence-driven world.

But ethics are only half the story. Competence in the age of artificial intelligence requires not just safeguards, but also mastery of the tools themselves. That next step will be the focus of the companion series, *Prompt Engineering for Lawyers*, which will demonstrate how attorneys can structure prompts, assign personas, refine outputs, and stress-test arguments to use artificial intelligence productively and competently. If the ethics series has shown that resistance to artificial intelligence is futile, the next series will show how lawyers can be empowered to direct, rather than be directed by, this technology.

APPENDIX A

Model Law Firm Policy on the Responsible Use of Artificial Intelligence

Effective Date: [Insert Date]
Firm: [Insert Name]
Applies To: All lawyers, paralegals, professional staff, contractors, and temporary personnel (**"Personnel"**).

Purpose and Scope. This Policy establishes governance, procedures, and safeguards for the responsible use of artificial intelligence (**"AI"**) tools in the delivery of legal services. Its objectives are to:

Ensure AI use complies with all applicable rules of professional conduct;
Protect client confidences and privileged information;
Preserve the accuracy, quality, and integrity of Firm work product; and
Promote the competent, ethical, and transparent adoption of AI in legal workflows.

Definitions. The following definitions apply to this policy:

AI Tool: Any software or service that generates, classifies, recommends, predicts, or summarizes content using machine learning or similar technology.

Approved Tool: An AI Tool listed on the Firm's Approved Tools List after completion of the vetting process described in Section 5.

Confidential Information: Client confidences, privileged materials, proprietary Firm information, and any personal or sensitive data protected by law, regulation, or contract.

Policy Supervisor: [Individual or Committee responsible for overseeing this policy]

Guiding Principles. The following guiding principles govern all use of AI by this Firm and all Personnel:

Augment, Don't Replace: AI supports, but does not replace, independent professional judgment.

Protect Confidentiality: Confidential Information may not be entered into any AI Tool unless safeguards are in place to prevent unauthorized retention, disclosure, or use.

Verify All Outputs: All AI outputs must be independently reviewed for accuracy, authority, completeness, and suitability.

Maintain Accountability: Attorneys remain professionally responsible for work product that incorporates AI outputs.

Honor Client Instructions: Attorneys remain professionally responsible for work product that incorporates AI outputs.

Engagement Letter: All engagement letters must include a Firm-approved disclosure regarding the potential use of AI tools in providing legal services. The lead attorney should provide a copy of the approved disclosure to clients who mandate the use of their own engagement letter.

Governance and Responsibilities.

Policy Oversight: The Policy Supervisor will oversee implementation of this Policy, maintain the Approved Tools List, conduct training, grant AI Tool-specific authorizations, and review incidents.

Tool Vetting: The Policy Supervisor will conduct the vetting process before any AI Tool is approved for use.

Matter Lead Attorney: For each client matter, the lead attorney will ensure AI use complies with this Policy and documented client instructions.

All Personnel: All Personnel must use only Approved Tools for which they have completed required training and received appropriate authorization.

Approved AI Tools List. No AI Tool may be used in client matters unless it is on the Firm's Approved Tools List. AI Tools are assigned to one of two categories:

General-Use Tools: These AI Tools are approved for use by all Personnel who have completed the Firm's baseline AI training. These tools have been vetted for broad application, low risk, and have built-in privacy and security safeguards that meet Firm standards.

Restricted-Use Tools: These AI Tools are approved only for designated, trained Personnel who have completed advanced AI

training, training on the specific AI Tool, and received written authorization from the Policy Supervisor. These tools may involve higher inherent risks (e.g., sensitive data handling, complex privacy configurations, advanced analytics affecting legal strategy) or require subject-matter expertise. Examples include: AI-assisted litigation strategy platforms, custom fine-tuned models containing proprietary or sensitive data, and advanced contract analytics platforms.

AI Tool Vetting Process. The vetting process for all AI Tools will include:

Terms Review: Reviewing the Terms of Service, Privacy Policy, and any applicable data agreements.

Privacy Safeguards: Confirming the ability to disable data retention and training on user inputs (or equivalent protections).

Compliance Review: Confirming consistency with professional responsibility obligations and applicable laws.

Appropriate User Level: Assigning each tool to either the General-Use or Restricted-Use category based on its features, risks, and training requirements.

Permitted Uses of Approved AI Tools. Personnel may use AI Tools only if they are on the Firm's Approved Tools List, assigned to the user's authorization level, and used for appropriate purposes. Examples include:

Drafting or revising standard provisions, templates, or form documents;

Summarizing public records, transcripts, deposition testimony, or discovery materials;

Generating outlines, timelines, or checklists for internal use;

Brainstorming legal theories or arguments;

Conducting preliminary legal research, provided that all results are verified against authoritative sources.

AI must always be used in a manner that supports, rather than replaces, the professional judgment of the responsible attorney.

Prohibited Uses of AI Tools. The following uses of AI Tools are strictly prohibited unless expressly authorized in writing by the Policy Supervisor:

Inputting Confidential Information into a tool that retains or trains on user data without approved safeguards;

Relying on AI-generated citations, quotes, or legal authorities without primary-source verification;

Allowing AI to make legal conclusions, strategic recommendations, or filings without attorney review and approval;

Using AI in violation of client instructions, court rules, documented client instructions, or applicable rules of professional conduct;

Uploading privileged or sensitive information into AI Tools without confirming privilege-preservation measures; and

Creating any false or misleading information, documents, images, or citations.

Client Communication and Consent.

Disclosure Obligation: AI use must be disclosed to clients whenever required by law, contract, professional rules, or client preference.

Documentation: All client instructions limiting or prohibiting AI use must be documented in the matter file.

Fee Impact of Restrictions: Clients must be advised that restricting AI use may increase fees due to additional attorney or staff time.

Fee Impact of AI Tool Use: Clients must also be notified in advance if the Firm intends to charge additional fees for using an AI Tool that will result in a separate cost (e.g., pay-per-use, subscription-based, or licensed premium features billed to the client). Such costs must be described clearly, including the basis for the charge and an estimate where feasible.

Verification and Quality Control. All outputs from AI Tools must undergo human review before being used externally. The responsible attorney must ensure that:

Citations are verified against authoritative primary sources;

Factual statements are confirmed against the record or other reliable sources;

Tone, format, and style comply with the intended audience's expectations (e.g., court, client, opposing counsel);

Logical and substantive accuracy meets the same standards required for non-AI work product; and

Unsupported or speculative content is removed or replaced with verified information.

Security Requirements.

Minimization: Share only the minimum data necessary for the intended task.

De-Identification: Where possible, paraphrase, anonymize, or mask sensitive information before input.

Privileged Material: Privileged content may only be processed using AI Tools with contractual and technical measures to preserve privilege.

Access Restrictions: Limit tool access to personnel with a legitimate business need and proper authorization.

Authentication: Use strong passwords and, where available, multi-factor authentication.

Configuration: Privacy and security settings must be reviewed and configured before initial use and periodically thereafter.

Monitoring: Periodic reviews should ensure AI Tool settings remain compliant with Firm policy.

Incident Reporting.

Immediate Notification: Personnel must immediately report suspected misuse of AI, data breaches, security incidents, or violations of this Policy to the Policy Supervisor.

Investigation: The Firm will investigate all reports promptly, take corrective action, and notify clients or authorities where required.

Remediation: Following an incident, the Firm will review the circumstances and adjust tools, settings, training, or policy as needed.

Training and Competency.

Baseline Training: All Personnel must complete Firm-approved baseline AI training before using any General-Use Tool.

Advanced Training: Personnel must complete advanced AI training, plus training on the specific AI Tool, before using any Restricted-Use Tool.

Curriculum Content: Training must cover effective and ethical use, prompt design, verification procedures, confidentiality, and security safeguards.

Ongoing Education: Annual refresher training is mandatory for all AI Tool users, and interim updates will be provided when significant legal, technological, or policy changes occur.

Policy Review and Continuous Improvement.

Annual Review: The Policy Supervisor will review this Policy at least annually to reflect changes in technology, law, professional standards, and client expectations.

Interim Updates: The Policy Supervisor may make interim updates to address evolving issues or urgent risks.

Feedback Loop: Lessons learned from incidents, audits, and training assessments will be incorporated into future policy revisions and training programs.

APPENDIX B

Model AI Training Program for Legal Professionals

Purpose: This program is designed to provide all personnel training necessary to use AI Tools competently, securely, ethically, and in compliance with the Firm's Policy on the Responsible Use of Artificial Intelligence (the **"AI Use Policy"**). The program is structured in two tiers:

Baseline AI Training: One session required for all users before they may use any General-Use Tool.

Advanced AI Training: Multiple sessions, tool-specific and role-specific, required before personnel may use any Restricted-Use Tool.

Tier 1: Baseline AI Training: General-Use Tools

Format: One-hour session, offered in person or virtual. Virtual training may be offered asynchronously.

Goal: Equip all Firm personnel with the essential knowledge and skills to safely and effectively use AI Tools approved for general use.

*Required F*or: All lawyers, paralegals, and staff before accessing any General-Use Tool.

Baseline Session Outline

Module 1: Introduction to AI in Legal Practice

What AI and large language models (LLMs) are.

Common legal applications and their limitations.

AI's role in supporting, but not replacing, professional judgment.

Module 2: Ethics and Firm Policy

Overview of relevant professional conduct rules (competence, confidentiality, candor, supervision).

Summary of the Firm's AI Use Policy and Approved Tools List.

Understanding the General-Use / Restricted-Use distinction.

Module 3: Safe Use Practices

Data minimization and de-identification techniques.

Recognizing prohibited uses.

Privacy and security settings for approved tools.

Module 4: Output Verification

Why verification is required.

How to check citations, facts, tone, and completeness.

Module 5: Client Communication Basics

When and how to disclose AI use.

Explaining client fee impacts from restrictions or premium tool use.

Tier 2: Advanced AI Training: Restricted-Use Tools

Format: Multi-session program tailored to the specific Restricted-Use Tool(s) and role of the user, offered in person or virtual. Virtual may be offered asynchronously.

Goal: Develop the advanced skills, judgment, and technical knowledge required to operate higher-risk AI Tools competently and ethically.

Required For: Any personnel seeking authorization to use a Restricted-Use Tool.

Session 1 Outline: Advanced Ethics and Risk Management

Purpose: To provide personnel with an in-depth understanding of the professional responsibility obligations, legal risks, and governance requirements involved in using higher-risk AI Tools.

Deep Dive into Professional Responsibility Rules

Rule 1.1 (Competence): How "technological competence" extends to AI use; examples from bar ethics opinions.

Rule 1.6 (Confidentiality): The difference between confidential and privileged information, and why AI use can jeopardize both if not properly safeguarded.

Rule 3.3 (Candor to Tribunal): The consequences of filing AI-generated work product without adequate verification.

Rule 5.1 / 5.3 (Supervision): How partners, managers, and supervisory lawyers are responsible for the AI use of those they oversee, including staff and junior attorneys.

Identifying Confidential, Privileged, and Sensitive Data

Categories of information requiring heightened protection (e.g., trade secrets, personal health information, personally identifiable information).

How to recognize metadata and embedded information that may be inadvertently disclosed.

Risk Categorization and Impact on Access Rights

How the Firm defines "General-Use" vs. "Restricted-Use" Tools.

Mapping ethical and contractual risk levels to tool authorization levels.

Examples of when to escalate for Policy Supervisor approval.

Privilege Preservation

Attorney-client privilege and work product doctrine in the AI setting.

Contractual and technical measures to ensure vendor tools qualify as "agents" for privilege purposes.

Avoiding privilege waiver through third-party AI processing.

Incident Scenarios and Liability Considerations

Case studies of AI misuse leading to sanctions or reputational harm.

Potential malpractice exposure and insurer requirements.

Responding to suspected breaches or policy violations.

Session 2: Advanced Prompt Engineering

Purpose: To enable personnel to design, refine, and control AI prompts that produce high-quality, relevant, and ethically compliant outputs for complex legal tasks.

Prompt Architecture for Legal Contexts

Breaking down complex legal questions into discrete sub-prompts.

Structuring prompts to clearly state the legal issue, jurisdiction, and factual context.

Using explicit instructions for format, scope, and tone.

Context Layering

Sequencing information in a way that minimizes risk of error or bias.

Feeding prior verified outputs back into the AI in a controlled manner to build complex analyses.

Handling sensitive information: when to mask, when to abstract, and when to exclude.

Precision Controls

Using qualifiers and constraints to avoid overly broad or speculative responses.

Requesting citations to specific authority and excluding non-authoritative sources.

Techniques to force the AI to acknowledge uncertainty or gaps in information.

Role and Perspective Simulation

Instructing the AI to assume a defined role (e.g., "act as opposing counsel," "act as a compliance officer") to stress-test arguments or documents.

Limiting role prompts to avoid misleading anthropomorphic interpretations of AI output.

Multi-Step Prompting for Accuracy

Iterative refinement: "draft → review → revise" cycles with explicit performance goals for each step.

Using verification prompts ("List all factual statements you made above and provide the source for each") to identify unsupported claims.

Error Trapping and Risk Mitigation

Designing prompts to surface assumptions, limitations, and potential counterarguments.

Identifying and correcting AI "hallucinations" at the prompt level.

Data Minimization Practices

Providing only the data elements strictly necessary for the AI task.

Abstracting, paraphrasing, or using hypotheticals to avoid disclosure of sensitive details.

Using pseudonymization and masking for client names and identifiers.

Session 3: Tool-Specific Technical Training

Purpose: To ensure personnel understand the features, configurations, and operational safeguards of the specific Restricted-Use AI Tool(s) they are authorized to use.

Note: Some Restricted-Use AI Tool providers offer customized training for their products. For certain AI Tools, the provider training may be substituted for this session or may be required in addition to this session at the direction of the Policy Supervisor.

Tool Overview and Capabilities

Overview of the tool's primary functions and intended legal use cases.

Distinctions between core features, optional modules, and advanced capabilities.

Known strengths (e.g., speed, advanced analytics) and limitations (e.g., accuracy in niche jurisdictions, handling of large datasets).

Examples of tasks where the tool should and should not be used based on risk, complexity, and client requirements.

Initial Setup and Access Controls

Account creation process, licensing requirements, and authentication.

Assigning role-based permissions aligned with the user's Firm authorization level.

Configuring initial settings to default to Firm-approved privacy and security configurations.

User Interface and Workflow Integration

Navigating the dashboard, menus, and workspace views.

Creating, saving, and retrieving projects or workspaces within the tool.

Integrating with Firm systems, document management platforms, and collaboration tools.

Import/export processes, supported file formats, and how to ensure compatibility with Firm templates and style guides.

Security and Privacy Settings

User Interface and Workflow Integration

Navigating the dashboard, menus, and workspace views.

Creating, saving, and retrieving projects or workspaces within the tool.

Integrating with Firm systems, document management platforms, and collaboration tools.

Import/export processes, supported file formats, and how to ensure compatibility with Firm templates and style guides.

Data Handling Protocols

User Interface and Workflow Integration

Navigating the dashboard, menus, and workspace views.

Creating, saving, and retrieving projects or workspaces within the tool.

Integrating with Firm systems, document management platforms, and collaboration tools.

Import/export processes, supported file formats, and how to ensure compatibility with Firm templates and style guides.

Audit and Logging Features

User Interface and Workflow Integration

Navigating the dashboard, menus, and workspace views.

Creating, saving, and retrieving projects or workspaces within the tool.

Integrating with Firm systems, document management platforms, and collaboration tools.

Import/export processes, supported file formats, and how to ensure compatibility with Firm templates and style guides.

Vendor Support and Documentation

Accessing official vendor training materials, user guides, and FAQs.

Reporting technical or functional issues to vendor support, including what information can be shared without breaching confidentiality.

Escalating unresolved issues internally to the Policy Supervisor for resolution or tool reassessment.

Session 4: Verification for Complex Outputs

Purpose: To teach personnel how to critically evaluate and confirm the accuracy, reliability, and suitability of AI-generated outputs in high-stakes legal contexts.

Verification as a Professional Duty

How the Rules of Professional Conduct (1.1, 1.6, 3.3) and court rules require human verification of AI-assisted work.

Consequences of inadequate verification in litigation, transactional, and advisory matters.

Multi-Layer Fact-Checking

Cross-referencing AI outputs against the factual record in the matter.

Identifying and reconciling discrepancies between AI outputs and client-provided information.

Avoiding reliance on unstated or implicit assumptions in AI-generated content.

Cite-Checking and Legal Authority Validation

Verifying that all citations refer to genuine, controlling, and up-to-date authority.

Checking pinpoint citations for accuracy and contextual relevance.

Detecting fabricated ("hallucinated") citations and non-authoritative sources.

Logical and Analytical Review

Testing AI-generated legal reasoning for logical coherence.

Identifying circular reasoning, omissions, or unsupported conclusions.

Ensuring legal arguments are grounded properly in verified facts and applicable law.

Bias and Perspective Evaluation

Recognizing potential bias in AI outputs based on training data or prompt framing.

Adjusting prompts or verification methods to address identified bias.

Formatting, Tone, and Style Compliance

Ensuring outputs conform to court formatting rules or client-specific style guides.

Removing informal, speculative, or non-legal language from drafts.

Maintaining a professional tone and avoiding anthropomorphic language that could mislead.

Risk Flagging and Escalation

Identifying outputs that require subject-matter expert review before use.

Determining when to involve the Policy Supervisor for additional oversight.

Documenting verification steps for high-risk or external-facing work.

Recertification Policy

Annual Recertification Requirement

All personnel authorized to use any AI Tool must complete annual recertification to maintain access rights.

Recertification ensures that users remain current with changes in Firm policy, applicable law, ethical standards, and tool functionality.

Recertification training may take the form of a condensed refresher program.

Scope of Recertification

General-Use Tool Users: Must complete the Baseline AI Training refresher, including updated policy content, ethics developments, and lessons learned from Firm audits or incidents.

Restricted-Use Tool Users: Must complete updated advanced refresher training for each Restricted-Use Tool they are authorized to use, including any vendor-provided or vendor-required modules, and demonstrate continued proficiency.

Recertification Triggers Outside the Annual Cycle

Recertification may be required immediately if:

The AI Tool undergoes a major update affecting privacy, security, or core functionality;

There is a material change in relevant law, regulation, or professional conduct rules;

The Firm identifies significant misuse or noncompliance during audits; or

A client's Outside Counsel Guidelines or engagement imposes new requirements.

Documentation and Recordkeeping

The Policy Supervisor will maintain records of all certifications and recertifications, including dates, training modules completed, and tools authorized for use.

Failure to complete recertification by the stated deadline will result in suspension of AI Tool access until training is completed.

Revocation of Authorization

The Firm may revoke a user's authorization to access an AI Tool if the user fails to meet recertification requirements, demonstrates misuse, or fails to adhere to Firm policy.

Revocation decisions will be documented, and reinstatement will require retraining and reauthorization.