

AI Use Policy Template for Law Firms

Model Framework for Responsible AI Adoption

About This Template

This model policy helps law firms and in-house legal departments establish guardrails for the ethical and secure use of AI tools. It is designed as a practical starting point to align internal practices with ABA Model Rules 1.1 (Competence), 1.6 (Confidentiality), 5.3 (Nonlawyer Supervision), and guidance from ABA Formal Opinion 512 (2024).

Disclaimer: This document is for general educational purposes and should be adapted to your firm's specific bar, jurisdiction, and client-confidentiality obligations.

1. Purpose

To promote innovation while ensuring compliance with ethical and professional-conduct standards in all AI-assisted work across the firm.

2. Scope

Applies to all attorneys, paralegals, interns, contractors, and staff who use, procure, or manage AI tools for client matters, firm operations, or communications.

3. Core Principles

- Accountability: Lawyers remain fully responsible for outputs generated with AI tools.
- Confidentiality: AI must never compromise client privilege or protected data.
- Transparency: Disclose material AI use internally and, where relevant, to clients.
- Fairness & Non-Bias: Evaluate outputs for potential bias or unfair impact.
- Security & Compliance: Use only tools meeting firm-approved data-protection standards.

4. Acceptable Uses

- Drafting or summarizing legal documents, contracts, or correspondence (with human review).
- Supporting legal research, discovery, and due-diligence tasks.
- Generating internal memos, reports, or client communications.
- Enhancing administrative efficiency and knowledge management.

5. Prohibited Uses

- Entering confidential or client-identifying data into public or unvetted AI systems.
- Producing legal advice or filings without attorney supervision.
- Altering billing or trust-account data automatically.
- Using unapproved third-party AI tools for matter-related work.
- Creating deceptive, manipulative, or misleading outputs (including marketing content).

6. Data Protection & Confidentiality

- Use only firm-approved AI platforms meeting encryption (AES-256) and audit-logging standards.
- Client data must be anonymized or de-identified before use in AI workflows.
- Any external tool processing client data must have a signed Data-Processing Agreement (DPA) and, where required, client consent.
- Report any suspected data breach to IT Security immediately.

7. Oversight & Accountability

- All AI outputs must be reviewed and approved by a qualified professional before client delivery.
- Attorneys must apply independent legal judgment to verify accuracy.
- Periodic audits should assess bias, accuracy, and compliance with firm standards.
- Report issues or errors to the firm's designated AI Governance lead.

8. Training & Awareness

- All users must complete basic AI Awareness or Prompt Writing training prior to tool access.
- Annual refreshers are recommended as technology and rules evolve.

9. Governance & Review

- Maintain a registry of approved AI tools and use cases.
- Conduct periodic reviews for compliance and effectiveness.
- Update this policy as technology or bar guidance changes.

10. Accountability Statement

All personnel using AI remain personally responsible for ensuring that:

- AI is used in accordance with this policy.
- All outputs are verified for ethical and factual accuracy.
- Client trust, confidentiality, and professional integrity are preserved.

Appendix (Optional Resources)

- AI Use Case Approval Form (Template)
- Firm Data Protection Policy
- ABA Model Rules 1.1, 1.6, 5.3 Quick Reference
- AI Risk Assessment Checklist