

// DOC_ID: * RES_01 · LAW_FIRM_AI_USE_POLICY

// VERSION: 2026.04 · LAST_REVIEWED: 2026-04-27

Law Firm AI Use Policy

A working template for adopting generative AI in a US law firm without a Bar complaint, a sanctions order, or a malpractice letter. Comprehensive. Customizable. Free.

// HOW TO USE

This is a **working policy**, not a brochure. Copy the entire document into your firm's document management system. Do a global find-replace on every [FIRM], [ROLE], and [DATE] token. Take Sections 5, 7, 9, and 10 to your Managing Partner — they require firm-specific decisions. Adopt by partner vote. Distribute to every attorney and staff member. Re-review quarterly.

Drafted from **ABA Formal Opinion 512 (July 2024)**, the **State Bar of California Practical Guidance on Generative AI (November 2024)**, **Florida Bar Ethics Opinion 24-1 (January 2024)**, **Texas Committee on Professional Ethics Opinion 705**, the **Damien Charlotin AI Hallucination Cases Database (1,294+ cases as of March 2026)**, and the actual current Terms of Service of Harvey, Thomson Reuters CoCounsel, and OpenAI. Citations throughout. Verify against your jurisdiction before adopting.

// TABLE OF CONTENTS

01	Definitions
02	Scope & Applicability
03	Foundational Principles
04	Data Classification
05	Tool Classification & Approved Vendors
06	Approved Use Cases by Data Class
07	Prohibited Uses
08	Verification & Citation Protocol
09	Court Disclosure
10	Client Disclosure & Engagement Letter Language
11	Supervisory Responsibility (Rule 5.3)
12	Training Requirements
13	Incident Reporting
14	Audit Trail & Record-keeping
15	Billing & Fees (Rule 1.5)
16	Policy Review & Revision
17	Acknowledgment Form
18	Appendix A — ABA Opinion 512 Quick Reference
19	Appendix B — State Opinion Crosswalk (CA, FL, NY, TX)
20	Appendix C — 2025–2026 Sanctions Ledger
21	Appendix D — Vendor TOS Decoded (Harvey, CoCounsel, ChatGPT)

SEC_01

Definitions

For purposes of this Policy:

- **"AI" or "Generative AI"** means any software system that produces novel text, images, code, or other content in response to user prompts, including (but not limited to) large language models (LLMs), retrieval-augmented generation (RAG) systems, multimodal models, and AI agents. This Policy applies regardless of whether the AI is presented as "AI," "automation," "smart assistant," or any other label.

- **"Public AI"** means a Generative AI tool offered to the general public on standard consumer terms, where inputs may be (i) retained by the vendor, (ii) used to train or improve the vendor's models, or (iii) accessible to the vendor's personnel. Examples: free-tier ChatGPT, free-tier Claude, free-tier Gemini, Microsoft Copilot personal.
- **"Enterprise AI"** means a Generative AI tool offered under a contractual agreement that (i) prohibits the vendor from training on customer data, (ii) imposes a defined data retention period, (iii) provides for data deletion on demand, and (iv) is supported by a Data Processing Agreement (DPA) and security addendum. Examples: ChatGPT Enterprise, Claude for Enterprise, Microsoft 365 Copilot under enterprise license, Google Workspace AI under EDU/Enterprise license.
- **"Legal-Specialized AI"** means an Enterprise AI tool designed and marketed primarily for legal practice, with features such as integrated citation verification, jurisdiction awareness, and matter-aware retrieval. Examples: Harvey, Thomson Reuters CoCounsel, LexisNexis Protégé / Lexis+ AI, Spellbook, Casetext.
- **"Local-First AI"** means a Generative AI tool that processes data primarily on hardware controlled by the Firm or by the responsible attorney, where outbound transmission to a third party is limited to model inference calls under a no-retention contract. The case file itself never leaves the Firm's perimeter.
- **"Client Confidential Information"** has the meaning given in Rule 1.6 of the applicable Rules of Professional Conduct and includes all information relating to the representation of a client, regardless of source, whether or not labeled as confidential and whether or not the client has expressly designated it as such.
- **"Output"** means any content generated by a Generative AI tool, whether text, citation, summary, draft, table, image, or otherwise.

SEC_02

Scope & Applicability

This Policy applies to:

1. All attorneys, of counsel, contract attorneys, paralegals, secretaries, IT staff, marketing personnel, and any other personnel of [FIRM] .
2. All independent contractors, vendors, and outsourced service providers performing work for the Firm or its clients.
3. All Firm-issued devices and any personally-owned device used to access Firm systems or Client Confidential Information ("BYOD").
4. All work performed on behalf of any client of the Firm, regardless of practice area, jurisdiction, or matter.

5. All non-client work performed using AI in connection with Firm operations (marketing, business development, knowledge management, internal communications, hiring, etc.).

This Policy applies to AI use that occurs on Firm-licensed tools *and* AI use that occurs on personal accounts ("Shadow AI"). The fact that an attorney uses a personal ChatGPT account or a personal Claude account does not exempt that use from this Policy.

SEC_03

Foundational Principles

This Policy is grounded in six principles. Every other section of this Policy is an operationalization of one or more of these principles:

1. **The attorney is the final checkpoint.** AI does not practice law. AI does not sign briefs. The attorney who signs is responsible for every assertion under Rule 11, Rule 1.1, and inherent judicial authority. "*I relied on AI*" is not a defense; it is an aggravating factor. See ABA Formal Op. 512, at 10-11; *Mata v. Avianca, Inc.*, 678 F. Supp. 3d 443 (S.D.N.Y. 2023).
2. **Confidentiality is the default; AI use is the exception.** Under Rule 1.6, the duty to preserve confidentiality applies to *all* information relating to the representation, whether or not the client has marked it confidential. ABA Op. 512 confirms this duty extends to information input into a GAI tool. The lawful use of AI requires affirmative analysis of where data goes — not silence.
3. **Tool category determines what data may be used.** A tool that retains and trains on inputs is architecturally unsuited for privileged data. A tool that does neither, under contract, may be used for privileged data with informed consent. The decision is technical, not aspirational.
4. **Verification is non-delegable.** Every citation, every quotation, every assertion of fact derived from AI must be independently verified against a primary source. The verification protocol is set forth in Section 8.
5. **Disclosure is owed to clients and to courts.** ABA Op. 512 §§ 36-44 require informed consent for material AI use. Federal courts in 90+ districts have standing orders requiring disclosure. The default presumption is: *disclose*.
6. **The Firm bears institutional responsibility under Rule 5.3.** Vendor AI is non-lawyer assistance. Under Rule 5.3, the Firm must take reasonable measures to ensure that the conduct of any non-lawyer (including AI vendors) is compatible with the lawyer's professional obligations. See ABA Op. 512 §§ 50-58.

SEC_04

Data Classification

Before any AI tool is used on any data, the user must classify the data. The classification controls which tool category may be used.

CLASS	DEFINITION	EXAMPLES
D-1 Public	Information that is published, public-record, or otherwise lawfully available to anyone without restriction.	Reported case law, published statutes, public regulations, the Firm's marketing copy, public CLE materials.
D-2 Internal	Firm operational information not specific to any client matter. Treated as confidential to the Firm but not subject to Rule 1.6.	Internal CLE outlines, hiring rubrics, financial templates with no client data, knowledge-management notes scrubbed of client identifiers.
D-3 Confidential	Any information relating to the representation of a client. Subject to Rule 1.6 in full.	Client name + matter, case-strategy memos, client emails, draft pleadings, discovery materials, witness statements, factual investigation notes, billing narratives.
D-4 Highly Sensitive	Confidential information subject to additional regulatory, contractual, or judicial restrictions beyond Rule 1.6.	Sealed records, protective-order materials, PHI under HIPAA, PII subject to CCPA/GDPR, trade secrets covered by NDA, classified information, grand-jury materials, attorney-eyes-only discovery, child-welfare records.

When in doubt, classify upward. A user who is unsure whether information is D-2 or D-3 must treat it as D-3.

SEC_05

Tool Classification & Approved Vendors

The Firm classifies all AI tools into one of four tiers. Each tier corresponds to the maximum data classification with which the tool may be used.

TIER	EXAMPLES	MAX DATA CLASS	REQUIRED CONTROLS
T-X Prohibited	Free-tier ChatGPT (consumer), free-tier Claude.ai, free-tier Gemini, free-tier Copilot, free Perplexity, all "uncensored" or jailbroken open-weight models, any AI tool not listed in the Firm's approved vendor register.	D-1 only (and only after Firm-counsel review)	Use is generally prohibited. Limited exception: D-1 research where the attorney has formally requested an exception via Section 7.
T-1 Enterprise General	ChatGPT Enterprise, ChatGPT Team (with admin opt-out of training), Claude for Enterprise / Claude Team, Microsoft 365 Copilot (E3/E5), Google Workspace AI (Business+/Enterprise), GitHub Copilot Business.	D-1, D-2	Executed Enterprise Agreement, training opt-out confirmed, DPA on file, defined retention period, Firm-administered SSO/MFA.
T-2 Legal-Specialized	Harvey (Platform Agreement), Thomson Reuters CoCounsel, LexisNexis Protégé / Lexis+ AI, Spellbook, Casetext (legacy), Robin AI, Litera AI.	D-1, D-2, D-3	Executed Master Service Agreement, executed DPA, executed Business Associate Agreement (if PHI), SOC 2 Type 2, training opt-out, retention <30 days post-termination, citation verification feature available.
T-3 Local-First	On-device LLM deployments (e.g., the Firm's Knight Legal AI workstation, llama.cpp, MLX-served models), self-hosted RAG systems with no-retention model API.	D-1, D-2, D-3, D-4	Documented architecture audit, encryption at rest, no-retention model API contract, audit log of every query, IT-administered access control.

// CRITICAL – READ BEFORE APPROVING

Tool classification is **not** the same as vendor reputation. Harvey is a respected legal-AI vendor; ChatGPT Enterprise is from OpenAI, also respected. The classification reflects *what the vendor's contract allows them to do with your data*, not the vendor's brand.

Read the actual Master Service Agreement and DPA before classifying any tool. Marketing claims on a vendor's website do not constitute contractual commitments. See Appendix D for decoded clauses from major vendors' current TOS.

Approved Vendor Register

The IT department maintains the Firm's authoritative Approved Vendor Register at [INTERNAL_URL] . Use of any AI tool not listed in the Register is prohibited. The Register is reviewed quarterly by the AI Steering Committee (Section 16).

Adding a tool to the Register requires:

1. A written request from a partner identifying the proposed use case.
2. IT review of the vendor's current TOS, DPA, and security addendum (use the Knight CTO Vendor Evaluation Checklist or equivalent).
3. Formal Tier classification by the AI Steering Committee.
4. Execution of the required contractual controls.
5. Documentation in the Register of: vendor, tool name, version, Tier, max data class, contract effective dates, and IT contact.

SEC_06

Approved Use Cases by Data Class

The following matrix governs whether a given combination of data class and tool tier is permitted. Where the cell reads "Permitted with Conditions," the conditions in Section 8 (Verification) and, where applicable, Section 10 (Client Disclosure) apply in full.

	T-X PROHIBITED	T-1 ENTERPRISE GENERAL	T-2 LEGAL- SPECIALIZED	T-3 LOCAL- FIRST
D-1 Public	[N] Prohibited (default)	[Y] Permitted	[Y] Permitted	[Y] Permitted
D-2 Internal	[N] Prohibited	[Y] Permitted	[Y] Permitted	[Y] Permitted
D-3 Confidential	[N] Prohibited	[N] Prohibited	[Y] Permitted with Conditions	[Y] Permitted with Conditions
D-4 Highly Sensitive	[N] Prohibited	[N] Prohibited	[N] Prohibited (default; partner-level exception only)	[Y] Permitted with Conditions

Conditions for D-3 / D-4 use

1. **Informed client consent.** Per ABA Op. 512 § 35: "*merely adding general, boiler-plate provisions to engagement letters purporting to authorize the lawyer to use GAI is not sufficient.*" Use Section 10 language.
2. **Pseudonymization where feasible.** Where the AI use does not require client identifiers (e.g., a doctrinal research query, a stylistic edit), the user must replace party names, witness names, account numbers, addresses, and other direct identifiers with neutral placeholders before submission.
3. **Verification per Section 8.** Every assertion derived from the Output must be independently verified.
4. **Audit log entry per Section 14.**
5. **For D-4: documented written approval** of the responsible Partner *before* the use, attached to the matter file.

SEC_07

Prohibited Uses

The following are prohibited at all tiers, on all data, by all personnel, with no exception:

1. Submitting a brief, motion, declaration, or other court filing without independent verification of every citation against a primary source (Westlaw, Lexis, Bloomberg Law, the court's own docket, or the official reporter).
2. Representing AI-generated text as the original work of a lawyer or as the lawyer's own thinking, in any context where the audience would reasonably expect lawyer-original content (court filings, expert reports, sworn declarations).
3. Inputting Client Confidential Information (D-3 or D-4) into any tool classified T-X (free consumer AI).
4. Inputting D-4 information into any tool not classified T-3 without prior written Partner approval.
5. Using AI to draft, review, or analyze a matter for which the user has not been formally assigned, even where the user has technical access to the file.
6. Using AI to generate fabricated communications attributed to identifiable third parties (witnesses, opposing counsel, judges, clients), including for "training" or "demo" purposes.
7. Using AI to circumvent any restriction in a protective order, sealing order, NDA, or court-imposed limitation.
8. Using AI for any task subject to a client-specific AI restriction in the engagement letter or separate written instruction from the client. The Firm maintains a per-client AI restriction register at [INTERNAL_URL] ; check it before any AI use on a client matter.

9. Using AI to evaluate, score, or screen candidates for hiring (lawyers or staff) without prior approval of the hiring partner and the General Counsel of the Firm. EEOC enforcement guidance treats automated employment decision tools as a regulated category.
10. Bypassing the verification protocol (Section 8) in the interest of speed.

SEC_08

Verification & Citation Protocol

For any AI Output that will be (i) included in a court filing, (ii) included in a written legal opinion to a client, (iii) included in a transactional document, or (iv) relied upon for any legal advice given to a client, the responsible attorney must complete the four-step verification protocol below:

STEP 01 · SOURCE VERIFICATION

For every citation in the Output, retrieve the cited authority from a primary source — Westlaw, LexisNexis, Bloomberg Law, the court's own opinion (PACER, Westlaw, Lexis, the court's website), or the official reporter. **Do not** verify a citation by asking the same AI tool to confirm it. Schwartz did this in *Mata*; ChatGPT confirmed the cases existed; the cases did not exist; sanctions issued. See Appendix C, row 1.

STEP 02 · PINPOINT VERIFICATION

For every quotation in the Output, retrieve the actual text from the cited source and confirm it matches verbatim. AI tools paraphrase liberally and present paraphrases as direct quotations. The 2026 Cassata v. Macrina sanctions order in NY explicitly addressed paraphrase-presented-as-quotation as a Rule 11 violation. See Appendix C.

STEP 03 · HOLDING VERIFICATION

For every proposition for which a case is cited, read the cited portion of the case and confirm that the case actually stands for the proposition asserted. AI tools regularly cite real cases for propositions the cases reject. The standard is the same standard applied to junior associate work: would a competent attorney be willing to defend this characterization in front of the cited court?

STEP 04 · DOCUMENTATION

Document the verification in the matter file. At minimum: (i) tool used, (ii) date and time, (iii) user, (iv) general description of the prompt (do *not* reproduce confidential prompt text in unsecured logs), (v) for each cited authority, the verification source consulted. Use the audit log template in Section 14.

// 2026 REALITY CHECK

As of March 2026, the Damien Charlotin AI Hallucination Cases Database tracks **1,294+ documented court decisions involving AI-fabricated material**, with approximately 800 from US courts. The daily pace is now *five to ten new sanctioned hallucinations per day across US courts*. The largest single sanction to date is **\$86,000** (*ByoPlanet v. Johansson*, S.D. Fla. Aug. 2025); the next is **\$31,100** (*Lacey v. State Farm*, C.D. Cal. May 2025) against Ellis George + K&L Gates jointly. Am Law 100 firms are not exempt: Sullivan & Cromwell apologized to Chief Judge Glenn in April 2026 for ~28 erroneous citations in the *Prince Global* Chapter 15 matter.

SEC_09

Court Disclosure

As of April 2026, more than 300 federal judges and dozens of state-court judges have issued standing orders or local rules requiring disclosure of AI use in court filings. The orders vary materially. The user is responsible for determining the rule of the specific judge and court before any filing.

The Firm's IT department maintains an internal cross-reference at [INTERNAL_URL]. The cross-reference is best-effort; the canonical source is the judge's chambers and the court's local rules.

Default disclosure language

Where a court requires disclosure but does not prescribe the form, the following language is acceptable to most US courts that have addressed the issue (modeled on Judge Nina Y. Wang, D. Colo., effective Dec. 1, 2025):

// SAMPLE DISCLOSURE

The undersigned counsel certifies that generative artificial intelligence — specifically, [TOOL_NAME], accessed under [FIRM]'s enterprise license — was used in the preparation of this filing for the limited purpose of [describe: e.g., drafting an initial outline; summarizing the record for internal review; checking grammar]. All language drafted with the assistance of generative AI was personally reviewed by counsel of record. All cited authority was independently verified against the primary source. [CLIENT] was advised of and consented to such use.

Where disclosure is not required

Even where a court has no standing order, default to disclosure when (i) the AI use was material to the substantive content of the filing, (ii) the filing contains a representation of original analysis,

or (iii) the lawyer would consider disclosure if asked.

SEC_10

Client Disclosure & Engagement Letter Language

ABA Op. 512 distinguishes between AI uses that are routine and require no client-specific disclosure (e.g., grammar-check on internal emails, AI-assisted document indexing) and AI uses that require informed consent under Rules 1.4 and 1.6.

Informed consent is required where the AI use will involve (a) input of D-3 or D-4 data, (b) AI-generated work product delivered to the client as the lawyer's original work, or (c) AI use that would materially affect the client's evaluation of the lawyer's work. Boilerplate consent in the engagement letter is *insufficient*. ABA Op. 512 § 35.

Recommended engagement letter language (2026)

Insert the following as a standalone section of the engagement letter. Client must initial the section. The Firm maintains a separate, matter-specific written consent for any AI use that exceeds the scope of the general consent.

Use of Generative Artificial Intelligence.

The Firm uses generative artificial intelligence ("AI") tools in selected aspects of its practice. The Firm has classified the AI tools it uses, and uses each tool only with categories of information for which the tool's contractual terms provide adequate confidentiality protection. The Firm does not use free, consumer-grade AI tools (such as the public version of ChatGPT) with any information relating to your representation. Every assertion of fact and every legal citation derived from any AI tool is independently verified by an attorney before use in any document delivered to you, filed with a court, or relied upon for advice.

By signing this engagement letter, you acknowledge that the Firm may use generative AI tools for the following limited purposes in your matter: (i) document review and indexing, (ii) initial drafting of routine documents and correspondence, (iii) legal research support (subject to verification by an attorney), and (iv) administrative tasks such as scheduling and meeting summaries. **You may opt out of any or all of these uses by giving the Firm written notice.**

The Firm will obtain your separate written consent before using any AI tool to (a) analyze unredacted attorney-client privileged communications other than as part of the Firm's standard document-review workflow, (b) generate substantive legal analysis or strategy that will be presented to you as the Firm's original work, or (c) handle any information subject to a court protective order, sealing order, or other restriction.

The Firm will not pass through to you the cost of subscriptions to general-purpose AI tools used by the Firm. Where the Firm uses a matter-specific paid AI service that the Firm would not otherwise have incurred (for example, premium document-analysis services for a large discovery production), the Firm may charge the actual, documented cost as a disbursement, after notice to you. Time saved by AI use will be reflected in the Firm's invoices: the Firm will not bill you for hours not actually worked.

Client acknowledges this disclosure: [CLIENT INITIAL] Date: [DATE]

For matters with elevated risk

For matters involving D-4 data, regulated industries (healthcare, finance, defense, public sector), or sophisticated clients with their own AI procurement standards, use a separate written AI-use addendum that specifies the tools, the categories of data, the verification protocol, and the data-retention terms.

SEC_11

Supervisory Responsibility (Rule 5.3)

Under Rule 5.3, partners and supervisory attorneys are responsible for ensuring that the conduct of any non-lawyer assistant — including a generative AI tool used by an associate,

paralegal, or contract attorney — is compatible with the lawyer's professional obligations.

This means:

1. The supervising partner is personally exposed to discipline for AI errors in work product the partner signs. *See* ABA Op. 512 §§ 50-58; *Smith v. Farwell*, 2024 WL 668533 (Mass. Super. Feb. 12, 2024) (supervising lawyer fined \$2,000 for associate's AI hallucinations); *Lacey v. State Farm*, No. 2:22-cv-09438 (C.D. Cal. May 6, 2025) (\$31,100 against firms jointly).
2. "I did not know my associate used AI" is generally **not** a defense. The *Fletcher v. Experian* opinion (5th Cir. Feb. 2026) explicitly rejected this argument.
3. Each supervising partner must (i) confirm in writing each quarter that the associates and staff under their supervision have completed required AI training (Section 12), (ii) review at least one AI-assisted work product per quarter for compliance with this Policy, and (iii) report any non-compliance to the AI Steering Committee within 7 days.

SEC_12

Training Requirements

The Firm requires three tiers of mandatory AI training. No personnel may use any AI tool on Firm work until the applicable training has been completed and certified by [ROLE: e.g., the Director of Legal Operations].

TIER	AUDIENCE	CONTENT	FREQUENCY
Foundation	All personnel	What AI is and is not. The Firm's AI Use Policy. Data classification. Approved vs. prohibited tools. Reporting obligations under Section 13. ABA Op. 512 in plain language.	Within 30 days of joining; annual refresher.
Practitioner	All attorneys, paralegals, and any staff member who will use AI tools directly	Hands-on training with each approved tool. Verification protocol (Section 8). Court disclosure (Section 9). Client disclosure (Section 10). Hallucination recognition.	Within 60 days of joining; annual refresher; tool-specific refresher when a new tool is added to the Register.
Leadership	Partners, practice group leaders, supervising attorneys	Foundation + Practitioner content. Plus: supervisory obligations under Rule 5.3, Section 11 quarterly reviews, recent sanctions cases (Appendix C), regulatory developments.	Annual.

SEC_13

Incident Reporting

An "AI Incident" includes any of the following:

- Inadvertent input of Client Confidential Information into a prohibited tool.
- Discovery, in a filed document or document delivered to a client, of a fabricated citation, fabricated quotation, or factual assertion derived from AI without verification.
- Discovery that an associate, paralegal, or staff member has been using AI in violation of this Policy.
- Vendor notification of a security incident, data breach, or unauthorized access affecting an approved AI tool.
- Notification from a court, opposing counsel, or a client of suspected AI-generated material in Firm work product.

Any AI Incident must be reported to the Firm's General Counsel and to the AI Steering Committee within **24 hours** of discovery, regardless of whether the user believes the incident is material. Failure to report promptly is itself a violation of this Policy.

Containment protocol (first hour)

1. Stop the offending use immediately.
2. Preserve all evidence: the prompt, the Output, the file as it stood at time of submission, browser history, account logs.
3. Do *not* delete, edit, or "clean up" any artifact. Spoliation aggravates every kind of sanctions analysis.
4. Notify General Counsel by phone (not email).
5. If a court filing is implicated, draft a Rule 11 corrective notice for review by General Counsel within 24 hours.
6. If a client may have been delivered AI-generated material in violation of this Policy, do not communicate further with the client about the matter until General Counsel has approved a disclosure plan.

SEC_14

Audit Trail & Record-keeping

For every AI use on a client matter (D-3 or D-4), the user must create an entry in the Firm's AI audit log. Use the matter management system field labeled [FIELD_NAME] or, if unavailable, the standalone audit-log template at [INTERNAL_URL] .

Each entry must include:

1. Date and time (ISO 8601, including time zone).
2. User (timekeeper ID).
3. Matter ID.
4. AI tool name and Tier classification.
5. Data class submitted (D-1 / D-2 / D-3 / D-4).
6. Whether identifying information was pseudonymized (Y/N).
7. General description of the task (one line — *not* the prompt text).
8. Verification steps completed (Step 01 / 02 / 03 / 04 of Section 8).
9. Whether Output was used in a client deliverable, court filing, or internal-only.

The audit log is retained for the longer of (i) seven years from the date of the entry, (ii) the period of any applicable client document-retention obligation, or (iii) the limitations period for any cause of action arising out of the matter.

SEC_15

Billing & Fees (Rule 1.5)

Per ABA Op. 512 §§ 65-79 and the State Bar of California Practical Guidance (Nov. 2024):

1. Lawyers **may not** bill a client for time saved by AI use. If a task that would have taken 4 hours takes 30 minutes due to AI assistance, the bill reflects 30 minutes plus reasonable verification time.
2. Lawyers **may not** bill a client for time spent learning how to use an AI tool, except where the learning is matter-specific.
3. Lawyers **may** charge the actual, documented cost of a matter-specific AI service as a disbursement, after disclosure to the client. The cost of general-purpose AI tools used across many matters is overhead.
4. Where the Firm uses a flat fee or contingent fee, AI efficiency does not reduce the fee, but the lawyer must be able to demonstrate that the fee remains reasonable in light of the actual time and effort expended.

SEC_16

Policy Review & Revision

AI Steering Committee

The Firm's AI Steering Committee comprises: [NAMES OR ROLES] — at minimum, one Managing Partner, the Director of IT (or equivalent), the Firm's General Counsel (or ethics counsel), and one practice-group leader. The Committee meets quarterly.

Quarterly review

- **Q1:** Review and update the Approved Vendor Register. Survey staff on Shadow AI use.
- **Q2:** Review new state-bar opinions and federal court standing orders. Update Sections 9 and 10 as needed.
- **Q3:** Sample 3% of AI-assisted work product. Audit verification documentation. Report findings to all partners.
- **Q4:** Annual policy refresh. Incorporate the year's lessons. Roll out updated training.

Emergency revision triggers

The Policy is revised between quarterly cycles upon: (i) issuance of a new ABA Formal Opinion on AI; (ii) issuance of an AI ethics opinion by the Firm's primary state bar(s); (iii) a new federal court standing order in a court the Firm regularly practices in; (iv) any AI Incident at the Firm; (v)

any reported sanction in this Circuit involving AI; (vi) any material change in the TOS or DPA of an Approved Vendor.

SEC_17

Acknowledgment Form

// EMPLOYEE ACKNOWLEDGMENT

I, [NAME] , in my capacity as [ROLE] at [FIRM] , acknowledge that I have received, read, and understood the Firm's Law Firm AI Use Policy (Version [X.Y] , dated [DATE]).

I understand that:

- I may use generative AI tools only in compliance with this Policy.
- I am personally responsible for any AI-generated content I include in any work product, court filing, or client deliverable that I sign or transmit.
- I will complete the required AI training before using any AI tool on Firm work.
- I will report any AI Incident to the Firm's General Counsel within 24 hours of discovery.
- I will not use any AI tool not listed in the Firm's Approved Vendor Register on any data classification above D-1.
- Violation of this Policy may subject me to discipline up to and including termination, and may subject me to professional discipline by the relevant Bar authority.

Signature: [SIGNATURE] Date: [DATE]

APX_A

Appendix A — ABA Op. 512 Quick Reference

The American Bar Association Standing Committee on Ethics and Professional Responsibility issued **Formal Opinion 512** on July 29, 2024 — its first ethics opinion specifically addressing generative AI in legal practice. Key holdings:

RULE	HOLDING	CITATION
1.1 Competence	Lawyers must have a reasonable understanding of the capabilities and limitations of GAI tools they use. Need not be experts; must remain vigilant as tools evolve.	Op. 512 §§ 7-15
1.6 Confidentiality	Before inputting client information into a GAI tool, lawyers must evaluate the risks of disclosure or unauthorized access. Includes risks from vendor personnel, other customers, model training, and security breaches.	Op. 512 §§ 19-29
1.4 Communication	Where AI use is material, informed consent is required. Boilerplate engagement-letter consent is insufficient.	Op. 512 §§ 30-44
3.3 Candor to Tribunal	Lawyers must verify GAI output before submitting to a court. Hallucinated citations are sanctionable under Rule 11.	Op. 512 §§ 45-49
5.1 / 5.3 Supervision	Partners and supervisors are responsible for AI use by associates, paralegals, and contract personnel — and for the conduct of vendor AI tools as non-lawyer assistants.	Op. 512 §§ 50-58
1.5 Fees	May not bill for time saved by AI. May not bill for time learning AI (with limited matter-specific exceptions). Pass-through costs require advance disclosure.	Op. 512 §§ 65-79

APX_B

Appendix B — State Opinion Crosswalk

Selected state-bar guidance current as of April 2026. This crosswalk is informational only — verify against the current guidance of your state bar before relying on it.

STATE	KEY AUTHORITY	DISTINCT FEATURES
California	Practical Guidance for the Use of Generative AI in the Practice of Law (State Bar of California, Standing Committee on Professional Responsibility and Conduct, Nov. 2024)	Most detailed framework in the country. Treats vendor TOS evaluation as a Rule 1.6 obligation. Explicitly addresses prompt injection. Addresses anti-discrimination concerns from AI training data. Recommends "vetted list of approved AI tools." Imposes specific scrutiny on hourly billing models when AI reduces task time by 70-90%.
Florida	Florida Bar Ethics Opinion 24-1 (Jan. 19, 2024)	First major state-bar opinion. Four-pillar framework: confidentiality, oversight, fees, advertising. Treats AI as "non-lawyer assistance" under Rule 5.3. Requires disclosure when AI chatbots interact with prospective clients. Requires informed consent before inputting confidential data into a third-party generative AI program.
New York	NYSBA Task Force Report on AI (April 2024); NY State Bar Opinion 1240 (Aug. 2024)	Permits AI under existing rules without new regulation. Emphasizes "supervisory" duty under Rule 5.3 over disclosure. Cites <i>Park v. Kim</i> (2d Cir. 2024) on attorney verification.
Texas	Texas Committee on Professional Ethics Opinion 705 (Feb. 2025)	"Reasonable and current understanding" of the technology. No hourly fees for AI-saved time. Verification of every assertion derived from AI. Lawyer is responsible regardless of who or what does the original research.

APX_C

Appendix C — 2025–2026 Sanctions Ledger (Selected)

Selected sanctions and discipline involving AI hallucinations in court filings. Drawn from the Damien Charlotin AI Hallucination Cases Database (1,294+ cases as of March 2026), Bloomberg Law, ABA Journal, and direct review of the cited orders. This list is illustrative — not exhaustive.

DATE	CASE & COURT	TOOL	SANCTION	LESSON
Jun 2023	<i>Mata v. Avianca</i> , S.D.N.Y. (Castel, J.)	ChatGPT (consumer)	\$5,000 ea. + firm; mandatory CLE; client letter	The founding case. Asking the AI to confirm its own citations is not verification.
Nov 2023	<i>People v. Crabill</i> , Colorado Supreme Court	ChatGPT	1-year-and-a-day suspension	First AI-related attorney suspension. Lying to the court about AI use is the aggravator.
Jan 2024	<i>Park v. Kim</i> , 2d Cir.	ChatGPT	Grievance Panel referral; sanctions on appeal	Eight months after <i>Mata</i> : novelty is no longer a mitigating factor.
Feb 2024	<i>Kruse v. Karlen</i> , Mo. Ct. App.	Unidentified	\$10,000 + appeal dismissed	22 of 24 citations fabricated. State appellate court will dismiss for AI abuse.
Feb 2025	<i>Wadsworth v. Walmart</i> , D. Wyo.	In-house AI tool ("MX2")	\$5,000 ea.; pro hac vice withdrawn	Even Morgan & Morgan (42nd-largest US firm) and "in-house" AI tools are sanctionable.
May 2025	<i>Lacey v. State Farm</i> , C.D. Cal.	CoCounsel + Westlaw Precision + Gemini	\$31,100 jointly (Ellis George + K&L Gates)	Legal-specialized tools still hallucinate. K&L Gates is the 14th-largest US firm.
Jul 2025	<i>Johnson v. Dunn</i> , N.D. Ala.	Unspecified AI	Public reprimand + disqualification	Court explicitly noted that monetary sanctions are "ineffective at deterring." Disqualification is the new floor.
Jul 2025	<i>Coomer v. Lindell</i> , D. Colo. (MyPillow)	Copilot + Gemini + Grok	\$6,000; ~30 defective citations	Multiple consumer AIs used in parallel without verification.

DATE	CASE & COURT	TOOL	SANCTION	LESSON
Aug 2025	<i>ByoPlanet v. Johansson</i> , S.D. Fla.	Unspecified AI	\$86,000 + dismissal with prejudice	Largest AI sanction to date. Repeated AI misuse despite warnings = catastrophic.
Feb 2026	<i>Fletcher v. Experian</i> , 5th Cir.	Unspecified	\$2,500; published opinion	Lying about AI use after the fact = harsher penalties. Acceptance of responsibility matters.
Feb 2026	<i>Cassata v. Macrina</i> , NY Sup. Ct. (Suffolk)	AI + plagiarized brief	\$10,000; first sanctions chart for AI errors	Courts are now systematizing the penalty structure.
Mar 2026	Federal court, Oregon (per NPR/Charlotin)	Unspecified	\$109,700	New record sanction reported; details emerging.
Apr 2026	Sullivan & Cromwell — <i>Prince Global Holdings</i> , Bankr. S.D.N.Y. (Glenn, C.J.)	Unspecified	Pending; self-reported apology	Even the most prestigious firms are exposed. Self-reporting is the right play.

APX_D

Appendix D — Vendor TOS Decoded

This appendix decodes selected clauses from the current public Terms of Service of three major vendors, accessed in April 2026. Vendor terms change frequently — verify against the current TOS before relying on this analysis. Direct quotations are in italics; the Firm's interpretation follows each.

Harvey (Platform Agreement, Last Updated Jan. 9, 2026)

WHAT HARVEY SAYS IT DOES WITH YOUR DATA

Harvey's Platform Agreement provides: *"You retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data. You grant to Harvey and its Affiliates a non-exclusive, worldwide, royalty-free right to process the Customer Data and Your Input to*

the extent necessary to provide the Service to You or Your Affiliates, to prevent or address service or technical problems with the Service, or as may be required by applicable law."

Knight CTO interpretation: The license is broad on its face but narrowly tied to "providing the Service." This is appropriate. Combined with Harvey's separately-stated "no training on customer data" commitment in their public materials and DPA, the contractual posture is acceptable for D-3 use. Confirm the no-training language is in *your executed* DPA, not just the public marketing page.

LIABILITY CAP THAT NOBODY READS

Harvey's Platform Agreement caps data-breach liability at *"the greater of (x) two times the amount actually paid or payable to Harvey by You in the prior 12 months relating to Your use of the Service or (y) \$500,000"* — described as the "Data Breach Cap."

Knight CTO interpretation: \$500,000 is materially less than the typical insurance recovery floor for a privileged-data breach affecting a meaningful matter. For a 50-attorney firm paying ~\$700K/year, the cap is \$1.4M. For a small firm paying ~\$15K/year, the cap is \$500K. *Consider negotiating the Data Breach Cap upward, or confirming your malpractice carrier covers the gap.*

RETENTION

Per Harvey's "Understanding Retention Policies" support article: *"Workspace retention can be customized anywhere from 3 hours after the data is processed by Harvey to 30 days after your agreement with Harvey ends."* Defaults to 30-day-after-termination deletion. Vault retention, custom workflows, and matter numbers are *retained independently* of workspace retention.

Knight CTO interpretation: The Vault and custom-workflow retention exceptions are easily overlooked and survive workspace deletion. Audit which features are in use. Set the workspace retention to the minimum compatible with the Firm's working style — 7 days is usually adequate.

UPDATE MECHANISM

Harvey reserves the right to update the Terms unilaterally, but only with the following protection: *"in no event may Harvey update such Terms in a way that detracts from its obligations as agreed to in this Agreement with respect to Confidential Information, Customer Data, Customer Content, or security, without express written authorization from You."*

Knight CTO interpretation: Best-in-class. The lock-in on data and security terms is unusual and protective. Make sure your executed agreement does not waive this.

Thomson Reuters CoCounsel

Thomson Reuters publishes a "CoCounsel Drafting security and privacy" video and a separate Security Addendum but does **not** publish a single canonical TOS-decoded statement equivalent to Harvey's. Material terms are in the executed Master Service Agreement.

Required diligence before using CoCounsel for D-3:

1. Confirm the executed agreement contains a "no training on customer data" clause.

2. Confirm SOC 2 Type 2 certification is current (request the current report; do not rely on a logo).
3. Confirm the data residency clause if your client matter has jurisdictional restrictions.
4. Confirm the data-breach notification timeline.
5. Confirm what Thomson Reuters does with prompts and outputs after the session ends — and after termination.
6. Confirm whether CoCounsel's underlying model providers (which include OpenAI in the legacy Casetext-derived stack) inherit your no-training protection.

The *Lacey v. State Farm* precedent (C.D. Cal. May 2025): A team using CoCounsel + Westlaw Precision + Gemini received \$31,100 in sanctions. The court did *not* hold that the tools were defective; it held that *the lawyers' verification protocol was inadequate*. Use of a Tier-2 tool does not eliminate verification responsibility under Section 8.

OpenAI ChatGPT (Consumer Free Tier)

OpenAI's consumer Terms of Service govern use of the free and Plus tiers of ChatGPT. The relevant clauses for legal practice:

- OpenAI may use inputs and outputs **to train its models** unless the user opts out. The opt-out is accessible in user settings; it is not the default.
- OpenAI personnel may access prompts for safety review.
- Liability is capped at the greater of \$100 or the amount paid to OpenAI in the 12 months preceding the claim — i.e., effectively \$100 for free users, \$240 for Plus users.
- No DPA, no Business Associate Agreement, no SOC 2 commitment in the consumer terms.

Knight CTO interpretation: The consumer ChatGPT tier is architecturally and contractually unsuited for any data above D-1. ChatGPT Enterprise is a *different product* with materially different terms (no training, DPA, SOC 2, BAA available). Do not conflate the two.

The recurring "model improvement" trap

Multiple legal-AI vendors include language that sounds protective but is not:

- "*We do not use your data to train our foundation models*" — does **not** preclude use to train fine-tuned models, retrieval indexes, or "service improvement" models.
- "*Your data is encrypted in transit and at rest*" — addresses transport security but not access controls within the vendor.
- "*We are SOC 2 compliant*" — refers to a specific audit scope; the audited controls may not include the AI model serving infrastructure.
- "*Your data stays in [region]*" — may apply only to storage, not to inference compute.

Read the executed agreement, not the marketing page. The Knight CTO Vendor Evaluation Checklist (RES_02) provides a structured 60-question framework for this analysis.

Published by **Knight CTO** – Fractional CTO for the practice of law.
This document is provided as a working template, free for any law firm to use, customize, and distribute internally. It is not legal advice. It does not establish an attorney-client relationship. Verify every authority against your jurisdiction before adopting. The document is a snapshot of standards as of April 27, 2026; standards evolve continuously.

Source: <https://knightcto.com/resources/firm-ai-use-policy.html> ·
© 2026 Knight CTO · Walnut Creek, California