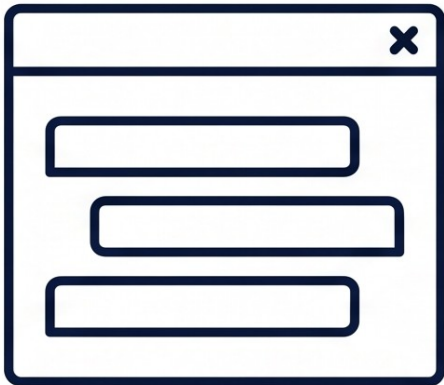




The Firm AI Policy Package

Chatboxes, Add-Ins, and Harnesses Under One Written Policy



THE CHATBOX



THE ADD-IN



THE HARNESS

John A. Kelly

Why a Written Policy, and Why Now

The standard of care moved in 2026; four drivers, none optional

**Fewer
than half**

of firms have a written
generative AI policy

COPRAC 2026 GUIDANCE

Rules 5.1 and 5.3: supervisors should establish clear AI policies, train staff, and keep the policies current.

Heightened duties for agentic tools.

COUNTY LOCAL RULES

Six counties adopted AI provisions effective 2026.

Santa Clara mandates disclosure in ex parte filings.

SB 574, PENDING

A personal read-and-verify duty in section 128.7, statewide.

Assembly deadline
August 31, 2026.

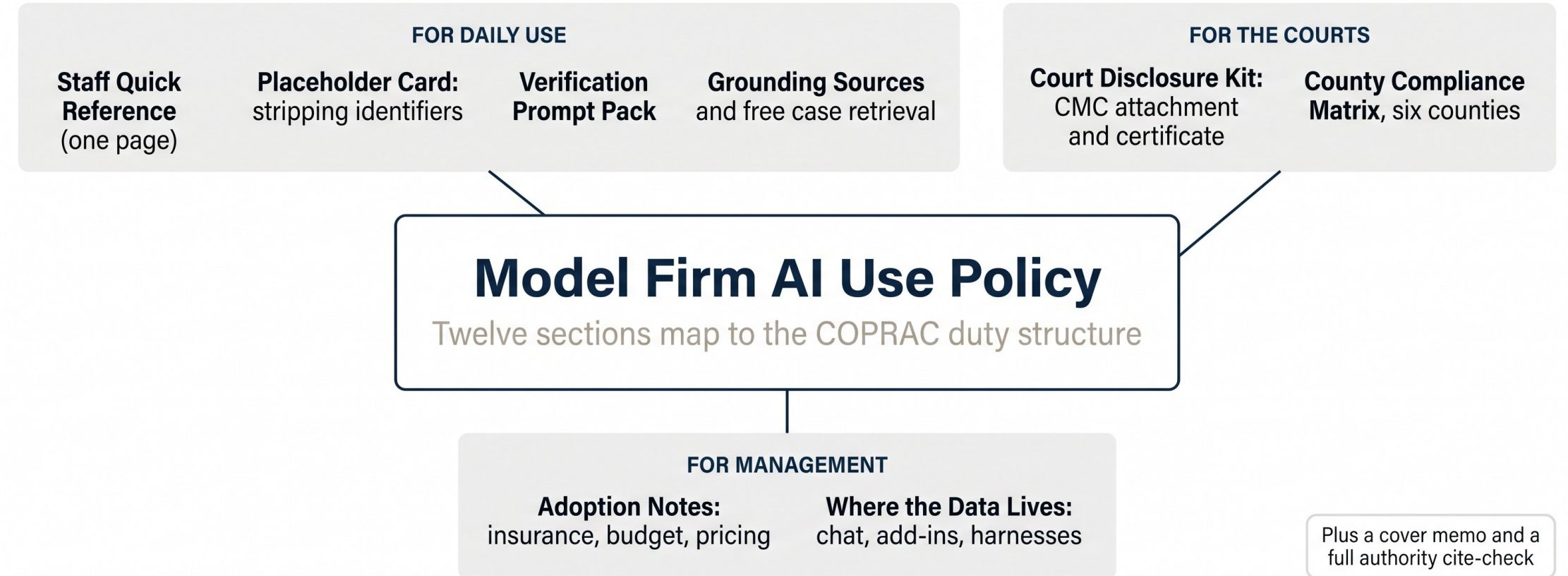
CYBER INSURANCE

Carriers now ask on applications: is there a written AI use policy?

A firm without a written policy is now visibly behind the standard of care. Fewer than half of firms have one; adopting now still reads as leadership, not catch-up.

What Is in the Package

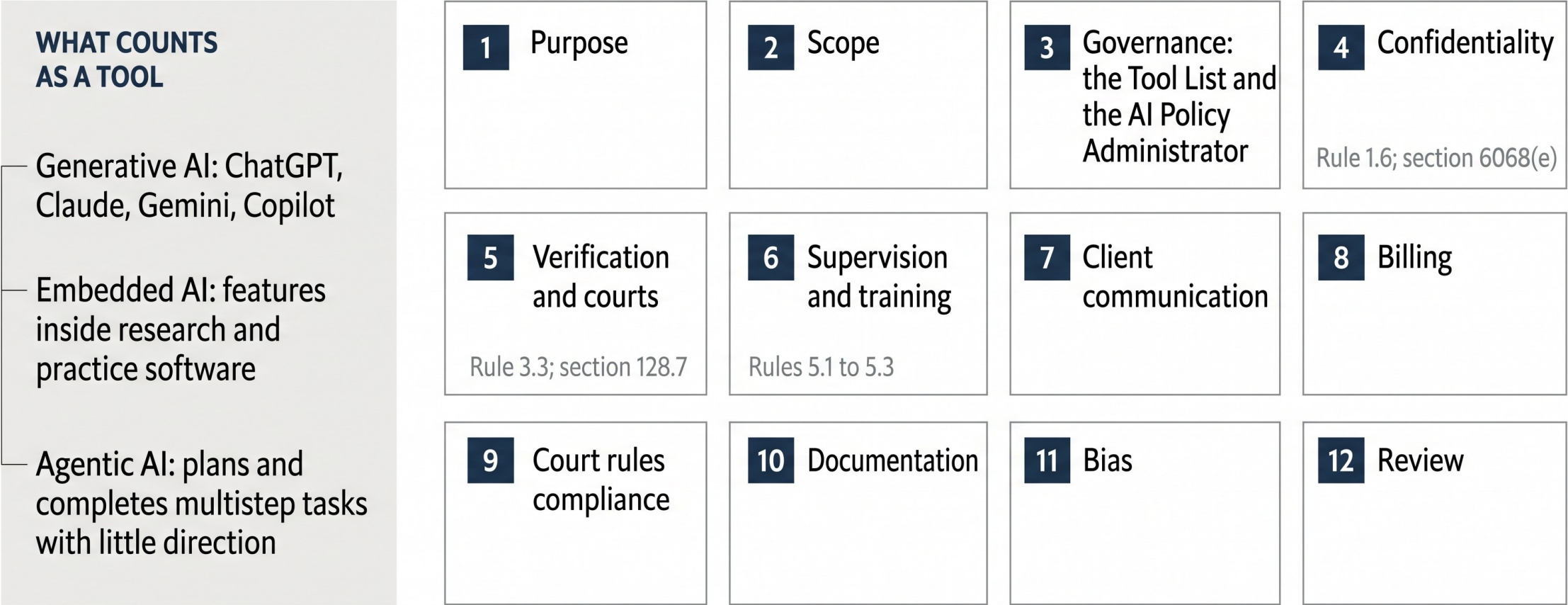
The policy states the duties; the companions do the daily work



Bracketed items mark the firm's decisions. A model to adapt with firm counsel; research assistance from one practitioner to another.

The Policy at a Glance

Twelve sections map to the COPRAC duty structure



The Approved Tool List is a one-page table at the back of the policy: each approved tool, its account and settings, and what the vetting found. If a tool is not on that page, it is not used for client work.

For Daily Use: The Documents by the Keyboard

The policy states the duties; these four documents carry the daily load

STAFF QUICK REFERENCE

One page, five moments: setup, before you type, research and drafting, before anything leaves the office, if something goes wrong.

PLACEHOLDER CARD

Strip client identifiers before anything goes to a cloud tool; the substitution key stays home.

The test: if opposing counsel read the prompt, would they know whose matter it is?

VERIFICATION PROMPT PACK

Ready-made prompts run the four-step citation ladder and build a claim inventory for facts.

The human pass stays with the responsible attorney.

GROUNDING SOURCES

Where official text lives, and how to pull a free copy of any cited case.

AI research startups resell the same free data; sources of record stay Westlaw, Lexis, or the official text.

Staff never need to read the whole policy to follow it. The one-page checklist and the placeholder card sit by the keyboard; the prompts and sources are ready when research starts.

For the Courts: The Disclosure Kit and the County Matrix

Three drafted instruments, and every county duty mapped with its effective date

THE COURT DISCLOSURE KIT

CMC Statement Attachment

Disclose **once** per case, where the court already surveys case management; names the accountable human on day one.

AI Disclosure Certificate

Optional, per filing, when the firm wants the record explicit.

Santa Clara Ex Parte Note

The one mandatory disclosure, with a model compliance sentence ready to adapt.

THE COUNTY COMPLIANCE MATRIX

Six counties adopted AI local rules effective 2026; the matrix states each duty and its date.

Only Santa Clara mandates disclosure, and only for ex parte material.

Everywhere else the duty is verification; check standing orders judge by judge.

Drafted from the July 2026 rule texts.

Voluntary disclosure is a posture choice; the kit makes it a one-page habit. The firm sets the default; the responsible attorney can depart from it for cause.

For Management: The Memos and the Cite-Check

What adoption costs, what to watch, and proof the authorities hold up

COVER MEMO

Why now, the tailoring steps, and the watch items, from one practitioner to another.

ADOPTION NOTES

Insurance questions, budget expectations, seat versus token pricing, and a training cadence that works.

WHERE THE DATA LIVES

The data-residence analysis the rest of this presentation walks through.

AUTHORITY CITE-CHECK

Every case, statute, rule, and local rule verified against Westlaw and the July 2026 texts.

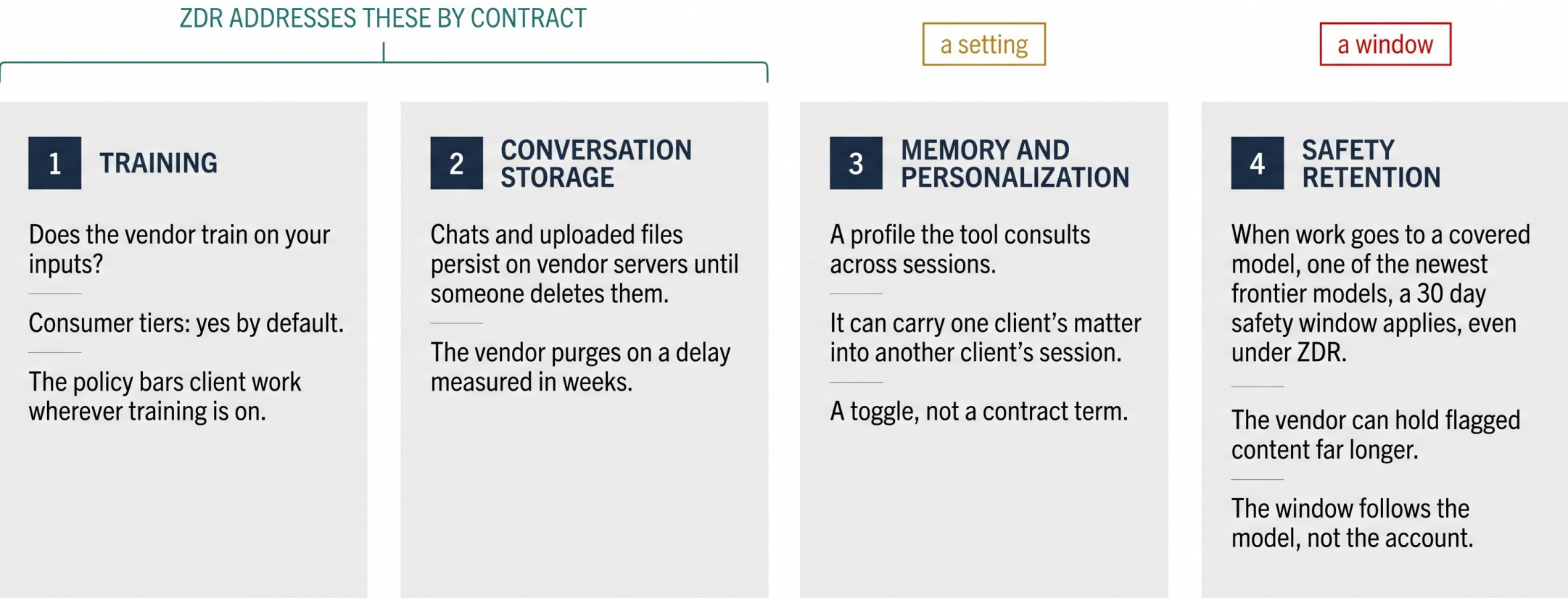
Result: one error found and corrected.

Nothing in the package rests on an unchecked citation. The full cite-check found one error, a CM-110 item number, and fixed it; the source downloads are filed as exhibits.



Four Things That Get Conflated as Retention

Zero data retention (ZDR) is a contract; it solves two of the four



A firm that gets ZDR terms and leaves memory on has solved the contract and kept the contamination.

Three Ways a Firm Actually Works With AI

Same vendor, three data footprints; the Tool List records the way of working, not just the tool



The chatbox

WHAT IT IS

A web chat interface:
type, paste, attach.

WHERE DATA GOES

Everything goes to the
vendor's cloud.

DISTINCTIVE RISK ■

Casual pasting; memory
on by default.



The add-in

WHAT IT IS

A vendor's AI program inside
Word, editing the open
document. Also sold as a plugin.

WHERE DATA GOES

The whole document goes
to the bound account.

DISTINCTIVE RISK ■

Disclosure that feels local;
silent edits.



The harness

WHAT IT IS

An agentic environment over
a folder the firm controls.

WHERE DATA GOES

Only the assembled context
goes to the model, over API.

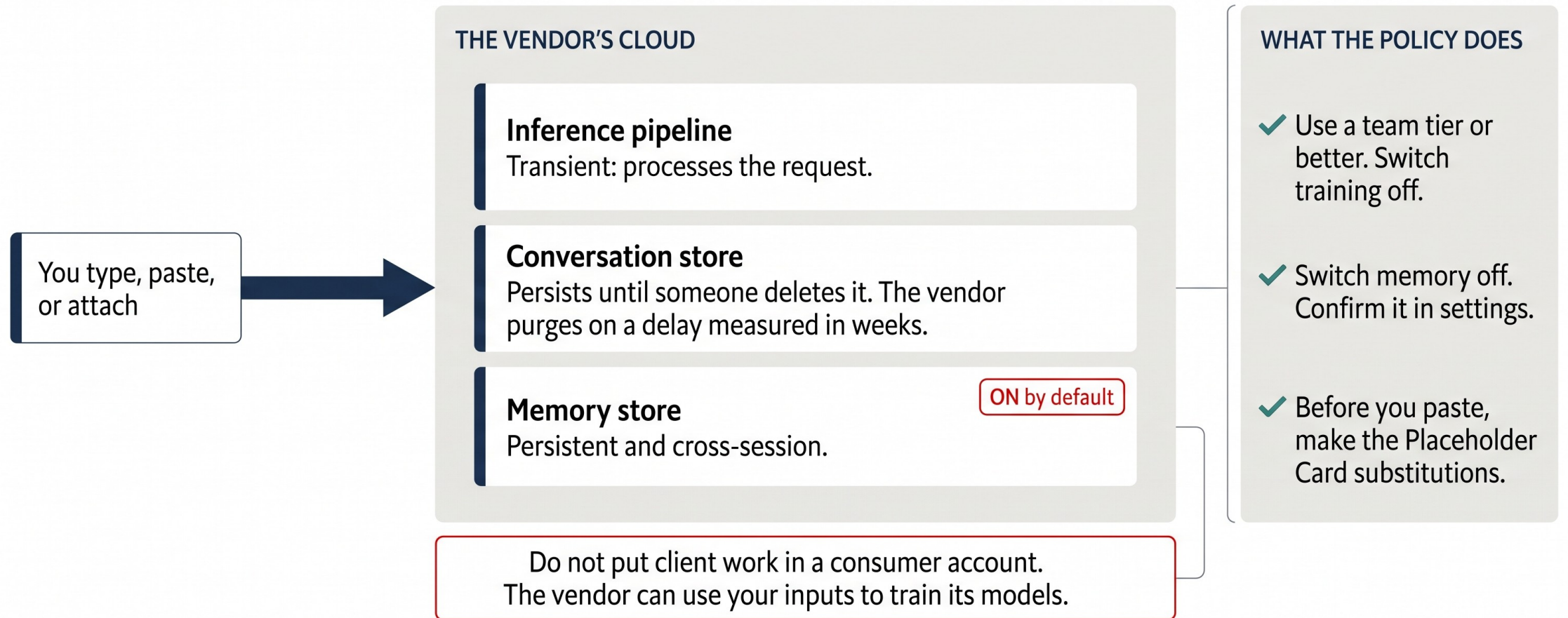
DISTINCTIVE RISK ■

Overbroad context;
autonomous action.

The ordinary-looking add-in has the hardest confidentiality profile; the exotic-looking harness has the most controllable one.

Way One: The Chatbox

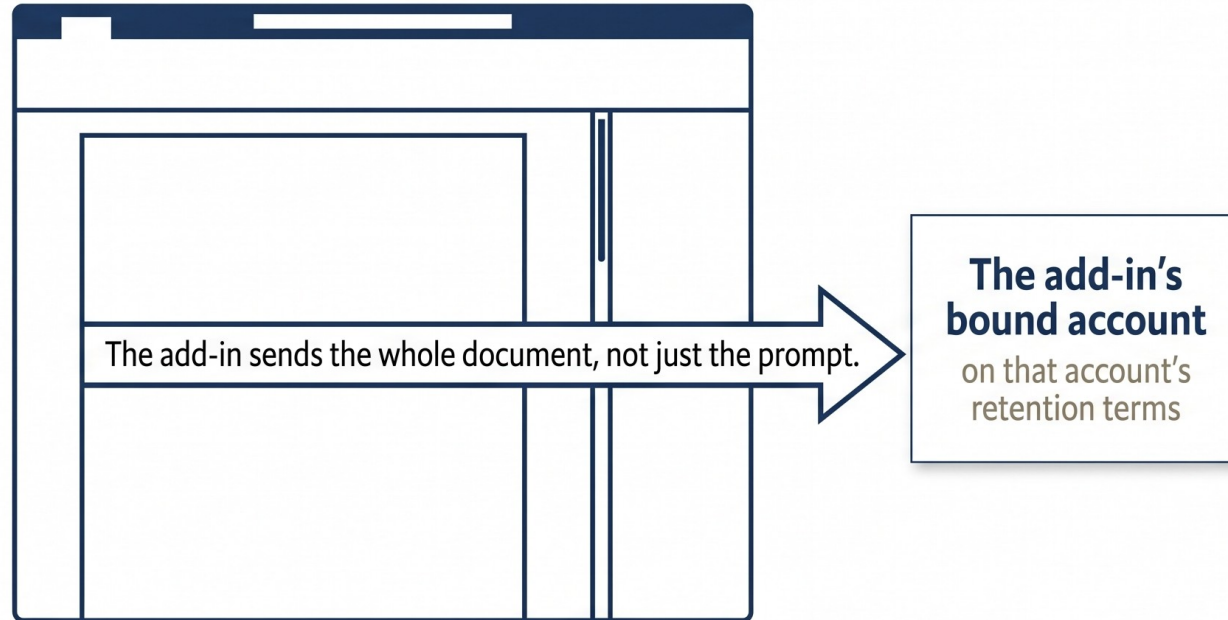
Everything typed or attached lands in the vendor's cloud, in three places at once



The only way of working where memory is routinely on by default. Team and business tiers are no-training with a stated retention period; they are not ZDR.

Way Two: The Add-In Inside Word

The Word window looks local. The document it shows is going to the vendor's cloud.



When the add-in is on, the unit of disclosure is the document: the prompt said fix the cross-references; the add-in sent the client agreement. A Tier 2 input: client documents, allowed only on enterprise-configured approved tools.

THE POLICY BARS SILENT EDITS

- Set the tool to edit in tracked changes.
- If it cannot, run the before and after versions through Word Compare.
- Review every change, not just the final text.

COPILOT: ONE MORE CLOUD VENDOR

- **Microsoft's cloud is not on by default:** Copilot is a sign-up, and Microsoft becomes one more vendor holding client data.
- **The credentials** that guard that data live outside the firm's own systems, and any cloud can be breached.
- **Not a harness either:** Microsoft picks the models, and the logs stay in Microsoft's cloud, not the matter file.
- **Vet Copilot like any vendor;** the decision goes on the Tool List, in writing.

The hardest ZDR of the three. When a document needs ZDR-grade handling, do not open it with a team-tier add-in.

Way Three: The Harness

The working set stays on firm ground; only the assembled context goes to the vendor

FIRM SIDE: THE WORKING SET



Matter documents
Standing instructions
Session logs

✓ The memory file: readable,
editable, scoped

Logs are attorney work product under section 2018.030. They stay in the matter file. Billing, troubleshooting, and section 10 documentation all read from one file.

only what
the session
assembles

VENDOR SIDE: PER REQUEST

The harness sends only the assembled context for each request, over API.

ZDR terms are most achievable on this channel.

■ If work routes to a covered model, a 30 day window still applies.

THE TWO EXPOSURES THE OTHERS LACK

You cannot see everything the agent reads. It can read more than you selected. Keep only one matter in the folder.

Autonomy: the same tool that edits can send or file. Do not let it file, send, or give client advice without human review.

Memory here is a file in the matter folder, not a vendor store. Keep one matter, one folder, one session. The tool cannot remember what was never in its working set.

ZDR in Practice: What the Contracts Actually Buy

A worked example with a real harness, and where the legal platforms stand

Worked example: Cursor with Privacy Mode on

- ✓ ZDR agreements with every model provider: the providers store nothing and train on nothing.
- ✓ The working set, logs, and memory stay in the firm's own folders. Billing and troubleshooting read from those logs, at zero vendor retention.
- **The exception:** if work routes to Anthropic's newest covered model, a 30 day safety window applies even under ZDR. The model stays off until an administrator accepts those terms. The window covers only the traffic that goes to that model.

THE LEGAL PLATFORMS, CHECKED AUGUST 2026

Harvey: puts it in the **standard contract**: model providers may not retain or record customer content, the **covered frontier model** is a contract **carve-out** an administrator must enable,

upload-first: every document it works on migrates to Harvey's cloud; Harvey deletes it within 30 days of termination.

Legora: the same clause, nearly word for word: no training, no retention, no human review,

no covered frontier model in its published stack, so no carve-out to accept, **the same** upload-first architecture, on Azure: the firm sets retention; Legora deletes within 30 days of termination.

The architectural price on both: record it on the Tool List at vetting. The firm's documents and its session logs stay in the vendor's cloud. No local logs exist, so billing reconstruction and troubleshooting run on the vendor's terms. The log you purge for confidentiality is the log you needed.

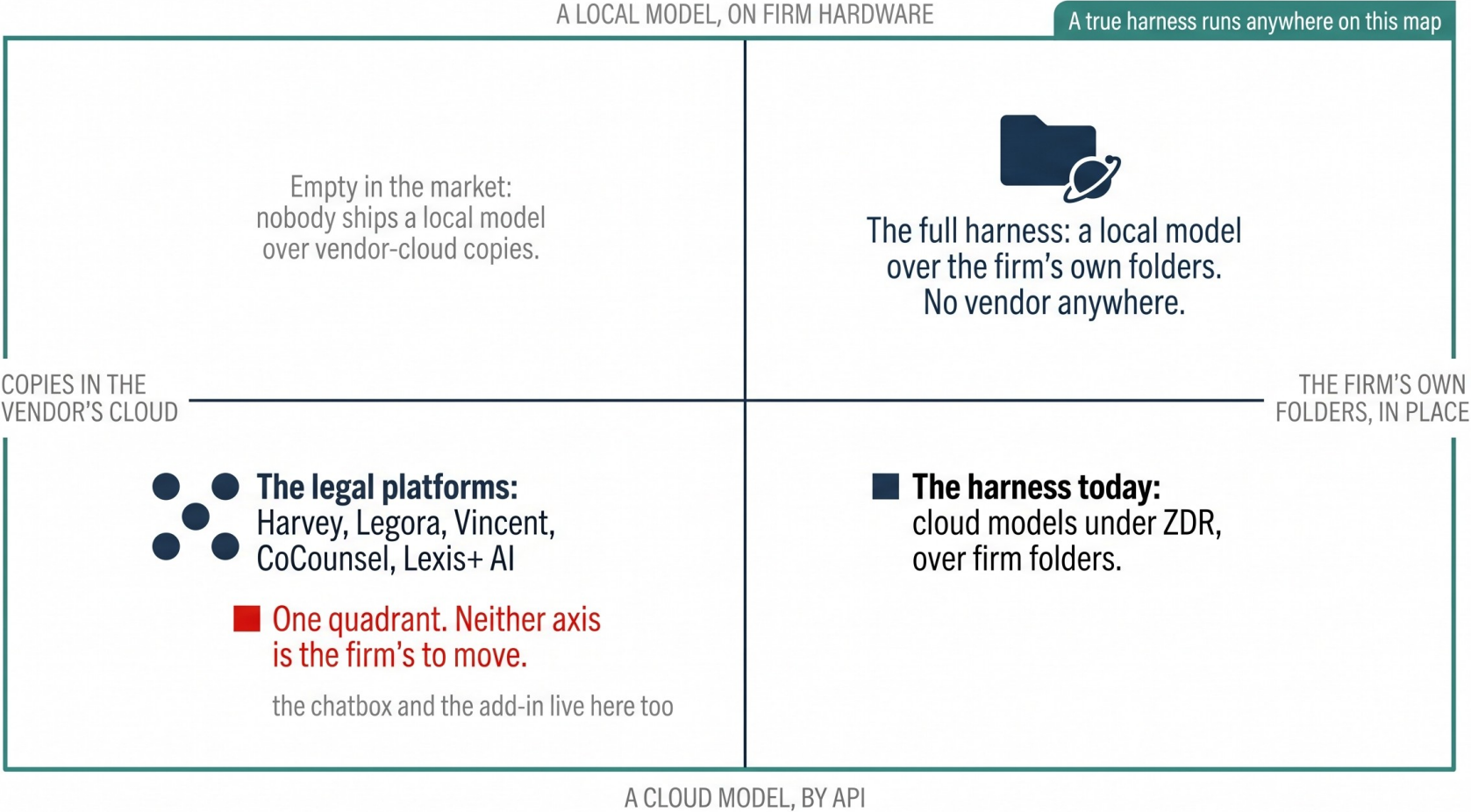
The vetting question is the same everywhere: which models, which windows, in writing, on the Tool List.

Contract stacks read in full, August 2026; the Tool List records what the signed order form says.

A harness under ZDR contracts works: zero retention for most models. The frontier-model window is a recorded, opt-in choice that follows the model, never a silent default.

What Counts as a Harness: The Four-Quadrant Test

Two axes of independence: who picks the model, and where the files live



THE WEAVING MILL, TWICE

1890
Every loom runs off one central shaft: first the water wheel, then the steam engine.

1900
An electric motor is bolted on where the wheel was. Same layout. No gain.

1920
A motor on every loom. The floor reorganizes. The gains finally arrive.

AI bolted onto a cloud document store is the motor where the wheel was.

Agentic behavior is a feature they host; a harness is a thing you hold. An agent inside the vendor's walls is the motor bolted on where the water wheel was.

The Platforms, Scored on What They Publish

Six tools, eight criteria: the harness test scored first, then the policy's vetting list

		harness benchmark						
		Cursor	Harvey	Legora	Vincent	CoCounsel	Lexis+ AI	
THE HARNESS TEST	MODEL: YOURS TO CHOOSE	Any cloud model, or a local one	The vendor's menu	The vendor's menu	The vendor's menu	OpenAI and Google only	The vendor's routing	
	FILES: IN PLACE	Yes, the firm's own folders	Upload-first	Upload-first	Upload-first	Upload-first	Upload-first	
	SESSION LOG: LOCAL	Logs live in the matter folder	Vendor cloud	Vendor cloud	Vendor cloud	Vendor cloud	Vendor cloud	
THE VETTING LIST	CONTRACT TEXT PUBLIC	Yes, with ZDR documents	Yes, full stack	Yes, full stack	Terms only	No; FAQ only	General terms only	
	NO TRAINING ON CLIENT WORK	In the contract	In the contract	In the contract	Marketing; the terms take a broad license	FAQ claim	Pledge with an improvement carve-out	
	MODEL PROVIDERS MAY NOT KEEP DATA	In the contract, every provider	In the contract	In the contract	Marketing claim	FAQ claim; abuse monitoring off	Not claimed	
	SAFETY WINDOW: 30 DAYS	Offered; admin opt-in	Offered; admin opt-in	Not in the stack	Not in the stack	Not in the stack	Unverified	
	VENDOR-SIDE MEMORY	None; memory is a local file	None	None	None claimed	None claimed	Yes: flagship feature, opt-out	

TEAL: VERIFIED FAVORABLE GOLD: PUBLISHED, NOT CONTRACT RED: NOT PUBLISHED, OR ADVERSE

Published postures as read August 5, 2026; Exhibits 01-10 in the matter file.

Only signed paper counts at vetting. A strong FAQ is an ask, not an answer. Ask the vendor to restate it in the order form. Then put the order form on the Tool List.

The Three Ways of Working in One View

Where the data goes, what persists, and where the policy carries the load

	Chatbox	Word add-in	Harness
CONTENT GOES TO	Vendor cloud	Vendor cloud, bound account	Vendor cloud, API channel
UNIT OF DISCLOSURE	What you type or attach	The open document	The assembled context
MEMORY LIVES	Vendor memory store; toggle off	The bound account; toggle off	✓ The matter folder; firm controlled
THE SESSION LOG	The vendor’s conversation store; if you purge it, you destroy the log	None the firm holds; account logs live with the vendor	✓ Local logs in the matter file: billing, troubleshooting, work product
ZDR AVAILABLE	Enterprise agreements only	Hardest of the three	Most achievable, API terms
DISTINCTIVE RISK	Casual pasting; memory on by default	Whole-document disclosure; silent edits	Overbroad context; autonomy

If you route to a covered model, a 30 day safety window applies even under ZDR, in all three ways of working. Non-covered models under ZDR retain nothing.

The safety window follows the model, not the way of working. If a client or a protective order cannot tolerate the window, use non-covered models under ZDR. Or have the section 7 conversation. Never use a workaround.

One Policy, Three Ways of Working

The same written duties, applied where each way of working needs them

	The chatbox	The Word add-in	The harness
THE TOOL LIST ROW SECTION 3	Vendor, account tier, approved configuration. Personal accounts are prohibited.	The bound account and its terms. An embedded AI feature is a tool; off until vetted.	The model stack and its ZDR terms, provider by provider.
REQUIRED SETUP SECTIONS 3 AND 4	Training off, memory off, team tier or better.	Tracked changes on; enterprise account for client documents.	Administrator approval, one matter per folder, audit logging, no autonomous sending.
CONFIDENTIALITY SECTION 4	Tier check before pasting; the Placeholder Card strips identifiers.	The tiers apply to the whole document, not just the prompt.	Substitution can happen in the folder, before anything transits.
VERIFICATION SECTION 5	The same duty in all three: the signing lawyer owns every citation. The four-step ladder, every time. No silent edits. Nothing files or sends itself.		
THE RECORD SECTION 10	Note tool, tasks, and verification in the matter file; export the session before you purge.	Keep the before and after versions; the compare redline is the record.	The session logs are the documentation and the billing entries, nearly free.

The policy names duties, not products. A new tool never means a new policy: it gets a Tool List row, a required setup, and the same duties as everything else.

Each Tool, on the Policy's Own Measures

The crosswalk applied: what vetting finds, tool by tool

	The Tool List row	Required setup	Confidentiality	The record	
	SECTION 3	SECTIONS 3 AND 4	SECTION 4	SECTION 10	
THE CHATBOX	ChatGPT or Claude, Team tier	Published terms; the Tool List records the tier's retention period.	Training off and memory off exist in settings; confirm both.	Tier 2, because the Tool List records the period. Not ZDR.	The vendor's conversation store; export before you purge.
	Microsoft 365 Copilot	Published enterprise protections; one more cloud-vendor row.	A sign-up, not a default; Microsoft picks the models.	Tier 2 in enterprise configuration; the whole document is the input.	Logs stay in Microsoft's cloud, not the matter file.
THE HARNESS	Cursor, Privacy Mode benchmark	Privacy Mode ZDR in published terms, provider by provider.	ZDR every provider; the covered model stays off until an administrator opts in.	Tier 2; identifiers can be substituted before anything transits.	Local logs in the matter file: billing, troubleshooting, work product.
THE PLATFORMS	Harvey	Contract read in full; no training, no retention, in the contract.	The covered-model carve-out is an administrator opt-in.	Tier 2 on contract terms; every document migrates to Harvey's cloud.	Upload-first: documents and session logs live in Harvey's cloud.
	Legora	The same clause, nearly word for word; contract read in full.	No covered model in the stack; no carve-out to accept.	Tier 2 on contract terms; the firm sets the Azure retention.	Upload-first: no local logs; billing runs on the vendor's terms.
	Vincent	Public terms take a broad license to user content.	The configuration the policy needs is not in the published terms.	No tier: an unvetted tool takes no client input.	Vendor cloud.
	CoCounsel	FAQ claims only; no public contract text.	ZDR APIs and abuse monitoring off, claimed at the FAQ layer.	Tier 2 only if the claims reach the signed order form.	Vendor cloud; no local logs.
	Lexis+ AI Protégé	No provider-ZDR claim; an improvement carve-out in the pledge.	Vendor memory is the flagship feature, an opt-out.	No tier on the published posture.	Vendor cloud.
	VERIFICATION SECTION 5	Rated nowhere because it changes nowhere: the ladder and the signing lawyer's duty are the same for every tool on this table.			

TEAL: VERIFIED FAVORABLE GOLD: PUBLISHED, NOT CONTRACT RED: NOT PUBLISHED, OR ADVERSE
Postures as read August 2026; Exhibits 01-10 in the matter file.

A rating is evidence, not endorsement. Teal is contract or verified terms, gold is a published claim, red is absent or adverse. The Tool List records which one the firm is relying on.

Confidentiality: Check the Tier, Then Strip the Identifiers

The sensitivity of the input, not the convenience of the tool, drives the choice

TIER 1, OPEN

Public information and anonymized hypotheticals.
Any approved tool.

TIER 2, CLIENT

Client documents and matter facts.
Enterprise-configured approved tools only.

TIER 3, RESTRICTED

Sealed, protected, or client-restricted material.
Stop. Ask the responsible attorney.

THE PLACEHOLDER CONVENTIONS

Parties: John Doe, Richard Roe

Witnesses: Peter Poe, Carl Coe

Property: Blackacre, Whiteacre

Entities: Acme Corp., Beta LLC

Numbers: [CASE NO.], [ACCT-1]

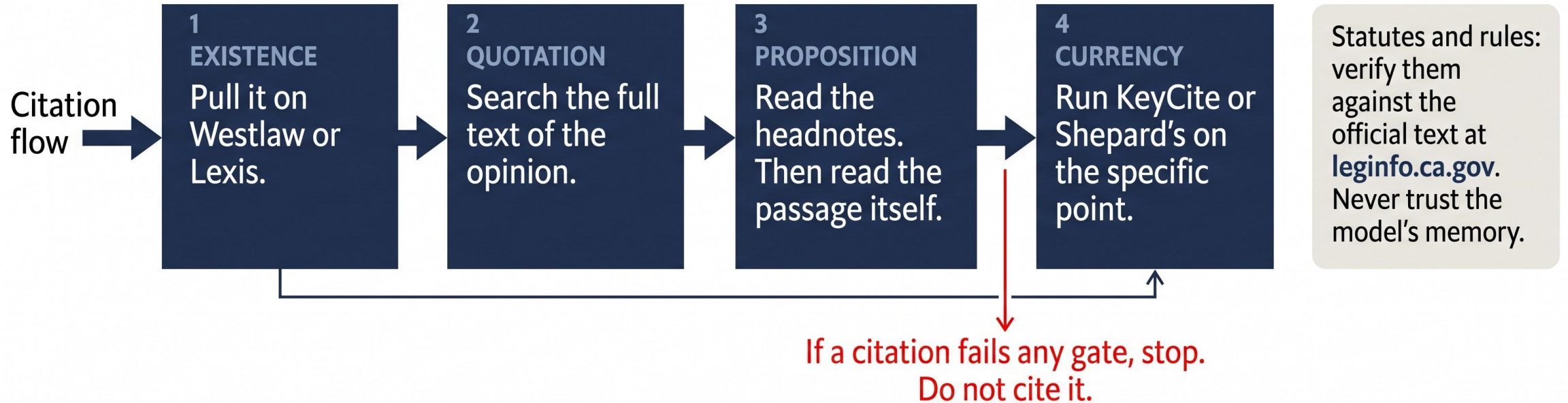
Preserve sequence and duration:
Day 1, Day 45, six months later.

Keep the substitution key in the matter file. Never paste it anywhere.

Pasting client text into a cloud tool to anonymize it is itself the disclosure. Substitute first. When in doubt, treat the input as Tier 3.
Ask the responsible attorney.

Verification: The Four-Step Ladder

The signing lawyer owns every citation, quotation, and contention; AI changes nothing



Mata v. Avianca, Inc.
(S.D.N.Y. 2023)
678 F.Supp.3d 443: fabricated cases, sanctions.

Noland v. Land of the Free, L.P.
(2025) 114 Cal.App.5th 426
[336 Cal.Rptr.3d 897]:
21 of 23 quotes fake, \$10,000.

United States v. Farris
(6th Cir. 2026) 171 F.4th 920:
unverified AI briefs; the court removed counsel.

Never trust a citation you did not verify. The sanctions cases got worse because of what came next. Correct the error first, always.

Courts: Six Counties Have AI Rules; One Mandates Disclosure

Two layers: the protocol disclosed once at the CMC, the section 128.7 signature on every filing

Santa Clara	Local General Rule 10, eff. 7/1/26	Disclose AI use in ex parte material. Review all AI-assisted submissions for accuracy and hallucinated output. disclosure duty
San Benito	Rule 10.3, eff. 1/1/26	Verification, non-delegable
San Mateo	Rule 2.14, eff. 1/1/26	Follow the court's posted AI expectations
Napa	Rule 3.10, eff. 1/1/26	Verification, non-delegable
Sacramento	Rule 1.28, eff. 7/1/26	Personally read and verify every citation
Mendocino	Rules 1.54, 1.55, eff. 7/1/26	Verification, non-delegable
All others, including Sonoma		Default duties; check standing orders, judge by judge

THE PROTOCOL LAYER, ONCE PER CASE

An attachment to the CM-110 case management statement.

Categorical disclosures; names the accountable human on day one.

Raise it first at the rule 3.724 meet and confer.

THE CANDOR LAYER, EVERY FILING

The section 128.7 signature governs each paper.

The CMC disclosure never immunizes a bad filing.

The kit includes an optional AI Disclosure Certificate for each filing.

Disclosed, verified use is the firm's public posture. If an error surfaces despite the protocol, the firm meets it as a documented outlier, not a concealment.

Running the Policy Day to Day

Supervision, training, billing, and the matter-file record

SUPERVISION

Supervisors own AI use by those they supervise.

No don't-ask-don't-tell: undisclosed tools are a violation.

The remedy for a Tool List gap is a proposal, not a workaround.

TRAINING

Onboarding, then a recurring short session.

One firm runs a half hour every Monday.

Rotate tool features, policy refreshers, sanctions cases.

BILLING

Bill actual time spent, never time the tool saved.

General subscriptions are overhead, like the library.

Optional task-unit pricing; the firm discloses it under section 6148.

DOCUMENTATION

Note tool, tasks, and verification in the matter file.

Cloud sessions leave no local log. Before you purge, export the session or note it in the matter file.

Harness session logs are that documentation, nearly free.

The same session logs that document verification generate the billing entries and the insurance answers. One habit, three payoffs.

Five Decisions to Tailor It, Two Things to Watch

Built so pending changes are citation updates, not structural ones

1 Name the AI Policy Administrator.

2 List the counties where you regularly file.

3 Take the honest tool inventory: which tools, which accounts, enterprise or personal.

4 Flag clients whose engagement terms restrict AI use.

5 Set the disclosure default: the CMC attachment in every litigated matter, or only where AI use is material.

WATCH ITEMS

SB 574 (Umberg): personal read-and-verify in section 128.7. Assembly deadline August 31, 2026.

COPRAC proposed comments to Rules 1.1, 1.4, 1.6, and 3.3. Trustees action expected later in 2026.

The honest inventory matters more than the aspirational one. What people actually use today, on which accounts, is where the policy starts.

Match the modality to the matter.

not just the tool to the firm

Memory is only solved where you can see it.
In a chatbox it is a setting to audit. In a harness it is a file to read.
Prefer the one you can inspect.

