



WHITE PAPER · REAL ESTATE BROKERAGE

Shadow AI in the brokerage, and what to do about it.

The question isn't whether your agents use AI. It's whether you know how they're using it.

EXECUTIVE SUMMARY

Your agents already use AI you have not approved, and you answer for what it produces.

Your agents and staff are already using AI tools you have not approved, and you are responsible for what those tools produce. That is shadow AI. It is not a future risk, because the adoption data shows it is the normal state of most brokerages today.

In 2026, 97% of brokerage leaders told Delta Media Group that their agents use AI.² In NAR's 2025 Technology Survey, ChatGPT accounted for 58% of the AI tools agents named, which suggests that much agent AI use runs through general consumer tools rather than tools the brokerage chose.³ Outside real estate, IBM found that one in five organizations it studied had a breach linked to shadow AI, and that those breaches cost about \$670,000 more on average.⁴

The broker's exposure does not depend on whether the broker knew. In Texas, for example, a broker is responsible for the authorized acts of sponsored agents and must keep written policies that make agents follow advertising rules and keep transaction records.⁵ An AI-written listing that steers buyers, or a client file pasted into a free chatbot, lands on the broker either way.

Banning AI does not solve this, because surveys consistently find that a large share of workers say they would keep using AI tools even under a ban. Ignoring it does not solve it either. This paper recommends a five-step path that brings AI use into the open instead of driving it underground:

1. **Find it.** Ask every agent and staff member which AI tools they use, under a short amnesty.
2. **Sort it.** Rank each use by the data it touches and whether its output reaches the public.
3. **Approve it.** Replace risky consumer tools with approved alternatives that do the same job.
4. **Set the rules.** Write the policy, review standards and records rules that cover the approved tools.
5. **Keep watching.** Repeat the inventory on a schedule, because new tools appear every month.

NAR's AI Policy Template for Brokers gives you the policy language for step 4. It does not do steps 1, 2, 3 or 5 for you, and it says plainly that it is not a failsafe against legal liability.¹ The rest of this paper explains why each step matters and how to carry it out.

This paper was written by NIRAP, which offers a governance and verification program for brokerages. Readers should weigh it with that interest in mind. Every factual claim is sourced in the notes at the end. Where a statement is NIRAP's own reasoning or characterization rather than an established fact, the text says so.

What shadow AI is, and what it is not

Shadow AI is any AI tool used for brokerage business that the brokerage has not reviewed and approved. NAR’s AI Glossary defines it as the use of unauthorized or unapproved AI tools by agents or staff, often without management’s knowledge, and says it increases security, compliance, fair housing and liability risks.¹

The definition turns on approval, not on the tool. The same tool can be shadow AI in one brokerage and approved in another. A paid business account with training switched off can be approved, while a free personal account of the same product is shadow AI.

THE BROKER’S REAL QUESTION

So the broker’s question is never “Is ChatGPT allowed?” The question is “Which account, for which task, with which data?”

Shadow AI in a brokerage usually looks ordinary. These are typical cases:

What the agent or staff member does	Why it is shadow AI
Pastes a seller’s disclosure into a free chatbot to summarize it	Client and transaction data went into a tool the brokerage never vetted
Writes listing descriptions in a personal AI account	Public advertising was drafted outside any review process
Uses a browser extension that rewrites emails	The extension can read every email it touches, including other clients’ details
Runs a phone app that records and transcribes buyer consultations	Client conversations are stored by a vendor with no contract with the brokerage
Virtually stages photos with a free image generator	Altered images may misrepresent the property and lack the disclosure MLS rules require
Asks a chatbot to estimate a home’s value for a client	A valuation reached the client with no record of how it was produced

Shadow AI is not the same as misconduct. Most people in these examples are trying to work faster and serve clients well. Treating them as offenders makes them hide the behavior, which is the opposite of what the broker needs. It is also not limited to licensed agents, because transaction coordinators, marketing staff and office managers handle the same client data.

How common it is

AI use in brokerages is close to universal, and most of it runs through consumer tools, so the realistic starting assumption is that shadow AI already exists in your firm. The figures below come from three different kinds of source, and each has limits worth knowing.

Finding	Source	What it measures
97% of brokerage leaders say their agents use AI	Delta Media Group, 2026 ²	Leaders’ reports on agents, 100+ brokerage leaders
Brokerages reporting no AI use fell from 24.8% in 2024 to 3.9% in 2026	Delta Media Group, 2026 ²	Same survey, three-year comparison
Data and security risks ranked as leaders’ top AI concern	Delta Media Group, 2026 ²	Same survey
68% of REALTORS® have used AI in their business; 20% use it daily	NAR 2025 Technology Survey ³	Agents’ own reports, 1,241 responses, July 2025
ChatGPT 58%, Gemini 20%, Copilot 15% of AI tools used	NAR 2025 Technology Survey ³	Which tools agents named
78% of workers who use AI bring their own tools to work	Microsoft and LinkedIn Work Trend Index, 2024 ⁶	Knowledge workers in 31 countries, not real estate
63% of organizations studied had no AI governance policy	IBM Cost of a Data Breach, 2025 ⁴	600 breached organizations, not real estate

The 68% figure is NAR’s survey arithmetic: 32% of respondents said they had not yet used AI in their business. NAR also found that agents spend their own money on technology, with 24% spending more than \$500 a month.³ That spending is the point. When an agent buys a tool personally, the brokerage usually has no contract with the vendor and no say in how the vendor treats client data.

The two surveys disagree on scale, and the reason matters. Delta Media asks brokerage leaders whether their agents use AI, and leaders tend to answer for the firm as a whole. NAR asks agents individually. Neither survey measures how much of that use the brokerage has approved, and no published real estate survey does. So the share of agent AI use that is shadow AI is unknown. What the data supports is narrower: agent AI use is common, consumer tools dominate it, and agents pay for many tools themselves.

Why agents and staff go around the broker

Shadow AI grows wherever the approved path is slower or missing, so the broker's first job is to understand the incentives rather than to assign blame. Four features of brokerage life make the incentives unusually strong.

The tools are free and already on the phone

A consumer chatbot takes seconds to open and costs nothing. An approved tool that needs a login, a request form or a wait for approval loses to it every time.

Agents run their own businesses

Most agents are independent contractors who choose and pay for their own technology. Many do not think of their marketing tools as the broker's business at all. NAR's template addresses this directly: it says independent contractors are still bound by the brokerage's AI policy when they act on the brokerage's behalf.¹

Workload pressure is real

In Microsoft and LinkedIn's 2024 study, 68% of workers said they struggle with the pace and volume of their work, and that pressure drives people to bring their own AI.⁶ Agents who write listings, answer leads at night and juggle transactions feel the same pressure.

People hide it

The same study found that 52% of AI users were reluctant to admit using it on their most important tasks.⁶ An agent who fears looking lazy or breaking a rule will not volunteer it. So silence from your agents is not evidence that shadow AI is absent.

The common thread is that shadow AI is mostly a supply problem. People reach for what works and what is available. A broker who supplies a good approved option and a clear rule removes most of the reason to go around it.

Where the risk shows up

Shadow AI creates risk in five places, and the supervising broker is answerable in all five. The first comes from how AI tools work; the other four come from existing law and rules that already apply to brokerage business, whatever tool produced the work.

AI's built-in flaws, with no one checking

Every generative AI tool shares three flaws. NAR's glossary describes the same hallucination and bias risks.¹

Hallucination The tool produces confident statements that are false, such as a square footage, a school assignment or an HOA rule that does not exist.	Sycophancy The tool tends to agree with the user and tell them what they want to hear, so an agent who asks "Is this price reasonable?" tends to get a yes.	Bias The tool carries bias from its training data, which in real estate can surface as steering language.
--	---	---

Approved tools have these flaws too. The difference is that approved use comes with a review step, and shadow use usually does not.

Client data leaves the brokerage

When an agent pastes a contract, a disclosure or a client's finances into a consumer tool, the brokerage loses control of that data. OpenAI, for example, lets users of personal ChatGPT accounts switch off a setting that allows their conversations to be used to train its models.⁷ An agent who has never opened that setting has not switched it off. NAR's FAQ lists the further problems: unapproved tools may store prompts, lack deletion guarantees, and create records outside the brokerage's control that could be subpoenaed.¹

1 in 5 organizations IBM studied attributed a breach to shadow AI	+\$670K average added breach cost where shadow AI was widespread	65% of shadow AI breaches compromised personal information	53% of all breaches IBM studied compromised personal information
---	--	--	--

Source: IBM Cost of a Data Breach Report 2025, 600 breached organizations across industries.⁴

Fair housing

The Fair Housing Act prohibits advertising that indicates a preference based on a protected class, and that prohibition applies regardless of who or what wrote the ad. An AI tool asked for a warm neighborhood description can produce phrases such as “perfect for young families,” which NAR’s template lists as prohibited examples.¹ The maximum civil penalties HUD’s administrative law judges can assess are set by regulation.⁸

\$26,262 Maximum civil penalty per violation, respondent with no prior violation	\$65,653 Maximum with one prior violation	\$131,308 Maximum with two or more prior violations
--	---	---

24 CFR §180.671. These amounts are adjusted for inflation and should be checked before you cite them.⁸

Misleading advertising and misrepresentation

AI-staged photos, invented features and confident but wrong descriptions are all advertising problems. NAR’s template says virtual staging must be disclosed and must not misrepresent the property, and that agents are responsible for everything in a listing even when AI drafted it.¹ In Texas, the broker must ensure a sponsored agent’s advertising complies with TREC’s advertising rules.⁵

Records and supervision

State licensing law already makes the broker answerable for agents’ work. Texas is a clear example, and other states have their own versions. Under 22 TAC §535.2:⁵

- The broker is responsible for the authorized acts of sponsored sales agents (subsection a).
- The broker may delegate supervision in writing but cannot give up overall responsibility for it (subsection e).
- The broker must keep written policies and procedures that ensure agents follow advertising rules and that records are maintained (subsection i).
- The broker must keep substantive communications with parties, and comparative market analyses, for at least four years (subsection h).

Shadow AI cuts across every one of these. A client email drafted and sent from a personal AI app, or a CMA produced in a chatbot, may never reach the brokerage’s records. The NAR FAQ makes the same point about litigation holds: prompts and outputs in unapproved tools may not be retrievable when they are needed.¹

A POINT THAT NEEDS CARE

No court or regulator has yet published a decision that turns on a brokerage's shadow AI specifically. The exposure described here comes from existing duties applied to a new tool, which is NIRAP's reading of those rules, not a ruling.

5 • THE EASY RESPONSES

Why banning AI and ignoring AI both fail

Brokers who notice shadow AI tend to pick one of two easy responses, and neither removes the risk.

A ban drives the use underground

In Software AG's survey, 46% of workers said they would refuse to give up their personal AI tools even if their organization banned them.⁹ A TrustedTech survey of 2,001 US and UK workers found the share willing to keep using AI under a ban ranged from 34% to 48% across the sectors it highlighted, even when discipline was possible.¹⁰ These are general workforce surveys, not real estate surveys, and self-reported intentions are not the same as behavior. Even so, the direction is consistent: a ban cuts the visible use and leaves much of the actual use in place. A ban also costs the brokerage the productivity gains its competitors are taking, and it makes agents less likely to report a mistake.

Ignoring it leaves the broker liable without a defense

The supervision duties described above do not pause because the broker chose not to look. A broker who has no policy, no list of approved tools and no review standard has nothing to point to when a regulator, a plaintiff or an insurer asks what supervision was in place.

The strongest counter-argument

Some brokers argue that a small firm with a few trusted agents does not need a formal program, and that a conversation at the sales meeting is enough. That position has real merit for a very small office, because the cost of a heavy program can exceed the risk. Its weakness is that it leaves no record. In Texas, written policies and procedures on advertising and records are already required whenever a broker sponsors agents.⁵ So the reasonable middle course is a program sized to the firm, not the absence of one.

GUARDRAILS, NOT BRAKES

The path that works sits between the two easy responses. It accepts that agents will use AI, and it makes the approved way the easiest way.

A five-step path out of the shadows

The goal is not zero AI use. The goal is that every AI use in the brokerage is known, sorted by risk, done in an approved tool and covered by a written rule. The five steps below run in a loop, because new tools keep arriving.



1 Find it, with an amnesty

Ask every agent and staff member to list each AI tool they use for work, what they use it for and what data they put into it. Announce a short amnesty window, for example 30 days, during which nothing reported leads to discipline. The amnesty is what makes the inventory honest. Without it, people report the tools they think you will approve and leave out the rest.

Keep the questions concrete. “Do you use AI?” gets a no from people who use a transcription app or an email plug-in and do not think of it as AI. Ask instead about listing descriptions, emails, social posts, photo editing, call notes, CMAs, contract summaries and lead follow-up, and ask which app does each.

2 Sort it by risk

Sort each reported use by two questions: what data goes in, and where the output goes. That gives three practical tiers.

Tier	What goes in	Where the output goes	What the broker does
High	Client personal or financial data, transaction documents, MLS data under license	Anywhere	Move to an approved tool now, or stop. NAR’s template treats putting this data into unapproved tools as a severe infraction
Medium	No client data	Public: listings, ads, social posts, client emails	Allow in an approved tool, with human review before anything is published or sent
Low	No client data	Internal only: brainstorming, generic research, drafting a training outline	Allow in approved or general tools; no special review

This tiering follows the structure of NAR's own one-pager, which limits general external tools to non-sensitive work and reserves sensitive data for approved tools.¹ The three-tier labels are NIRAP's simplification.

3 Approve replacements, not just restrictions

For every high-tier use you shut down, name an approved tool that does the same job. If agents use a free chatbot for listing descriptions, approve a business account or a vendor tool with a contract that bars training on your data, as NAR's template requires. If you only say no, the use returns in a different app within weeks, because the need that drove it is still there.

Keep the approved list short and public inside the firm, in an approved tool register that records each tool, its approved uses, the data it may touch and its contract status. A short list that agents actually know beats a long one that no one reads.

4 Set the rules in writing

Write down the policy, the review standard for anything public, and the records rule. The policy says which tools and which data. The review standard says who checks AI-drafted listings, ads and client messages for accuracy and fair housing language before they go out. The records rule says how AI-assisted communications and CMAs get into the transaction file so they can be produced later. NAR's template provides most of the policy language; the review standard and records rule must fit your own systems.

Pair the rules with short training, because a policy agents have not been walked through changes little. NAR's template calls for training at adoption, at onboarding and at least annually.

5 Keep watching

Repeat the inventory at least twice a year, and ask about new tools at every onboarding and every sales meeting where technology comes up. Make it easy to report a mistake, such as client data pasted into the wrong tool, and treat a prompt report better than a hidden one. NAR's template sets out tiered consequences, from retraining for minor lapses to escalation for uploading sensitive data. Use them, but keep the emphasis on bringing use into the open, because that is what lowers risk.

What NAR’s template covers, and what it leaves to you

NAR’s AI Policy Template for Brokers, released in March 2026, is the best free starting point for the rules in step 4, and it addresses shadow AI more directly than most brokers realize. It is also a template, not a program, so several steps remain the broker’s job. The table compares the two. The “covers” column paraphrases the template;¹ the “left to you” column is NIRAP’s reading.

Area	What the template covers	What it leaves to the broker
Approved tools	Only approved tools for brokerage business; an approved tools list kept by an AI Oversight Lead	Which tools go on the list, and who in your firm is the lead
Personal accounts	No personal or free consumer AI tools for client or internal brokerage data	Finding out who already uses them (step 1)
Sensitive data	Defines client, transaction and MLS data; bars it from unapproved tools; minimum necessary data	Training agents to recognize it in practice
Vendors	Contracts must bar training on brokerage or client data; keep a vendor inventory	Reading the contracts, and building the inventory
Human review	Required before AI content reaches a listing, a client, an ad, a transaction document or a CMA	Who reviews, how fast, and how the review is recorded
Records	Audit logs “where feasible”; litigation hold caution	How AI-assisted work gets into the transaction file your state requires
Independent contractors	Bound by the policy when acting for the brokerage	Getting agents to sign and follow it
Enforcement	Tiered infractions, from retraining to escalation	Applying them consistently, and an amnesty to start
Proof	Not addressed; the disclaimer says it is not a failsafe against legal liability	Evidence that the policy is actually followed

The last row is the gap that matters most for shadow AI. A policy states what should happen. It does not show what is happening. A broker who adopts the template word for word, files it and never checks has a document, not a program. The inventory, the register, the review records and the training records are what show a regulator, a court or an insurer that supervision took place.

Ten questions a supervising broker should be able to answer

If you cannot answer a question below with a document or a record, that question marks where shadow AI can live in your firm.

- ☐ Which AI tools do my agents and staff use for work today, and when did I last ask?

- ☐ Is there a written list of approved AI tools, and do my agents know where it is?

- ☐ For each approved tool, does the contract or account setting stop the vendor from training on our data?

- ☐ What client, transaction or MLS data are agents allowed to put into AI tools, and is that written down?

- ☐ Who reviews AI-drafted listings, ads and client messages before they go out, and is the review recorded?

- ☐ How do AI-assisted emails and CMAs get into the transaction file I must keep?

- ☐ Has every agent and staff member been trained on the AI policy, and do I have the training record?

- ☐ If an agent pasted client data into the wrong tool today, would they tell me, and do they know how?

- ☐ Have my delegated supervisors been told that AI use is part of what they supervise?

- ☐ When will I next repeat the inventory?

Limits of this paper

This paper is not legal advice, and a broker should have counsel review the final policy, as NAR's template also recommends. Four limits are worth stating plainly.

- **No real estate survey measures shadow AI directly.** The adoption figures measure AI use, and the ban and breach figures come from general workforce studies. The share of brokerage AI use that is unapproved is unknown.
- **The legal examples are Texas rules.** Other states impose similar broker supervision and records duties, but the wording and retention periods differ. Check your own state's rules.
- **Penalty amounts change.** Federal fair housing penalties are adjusted for inflation each year.
- **No decision yet turns on shadow AI.** The exposure described here applies existing duties to a new tool. It is a reasoned reading, not settled case law.

About NIRAP and RAICB™ certification



The National Institute for Responsible AI Practice (NIRAP) is a standards and certification body for professionals and firms that use AI.

For brokerages, NIRAP offers a program with three parts. The **Responsible AI Toolkit** produces the core documents described in step 4: an approved tool register, an AI policy, review requirements, records retention rules and a rollout plan. **AI Governance 101** is training for agents and staff. **RAICB™ certification** is independent verification that leads to the RAICB™ trust badge. NAR has shown brokers what to do. NIRAP verifies they have done it.

Details are at brokers.nirap.org. A free AI governance gap assessment is available at tools.nirap.org. Questions can be sent to contact@nirap.org.

NOTES AND SOURCES

Sources

All sources were opened or checked on October 23, 2026.

1. National Association of REALTORS®, AI Policy Template for Brokers (policy, AI Glossary, Agent & Staff FAQ and one-pager), March 2026. Public copy hosted by Bay East Association of REALTORS®. bayeast.org/wp-content/uploads/NAR-Brokerage-AI-Policy-Kit-March-2026.pdf
2. Delta Media Group, 2026 Real Estate AI & Leadership Survey (more than 100 brokerage leaders), as reported by HousingWire and Florida Realtors; three-year analysis press release, August 2026. housingwire.com/articles/brokerages-increase-ai-adoption-as-business-priorities-shift · floridarealtors.org/news-media/news-articles/2026/08/brokerages-expand-ai-use-safeguards-take-focus · norfolkdailynews.com/online_features/press_releases/real-estates-ai-opt-out-is-nearly-extinct-new-delta-media-analysis-finds

3. National Association of REALTORS®, “REALTORS® Embrace AI, Digital Tools to Enhance Client Service, NAR Survey Finds,” September 18, 2025 (2025 Technology Survey, fielded July 2025); tool shares as reported by GAAR; sample size and spending figures as reported by HousingWire. nar.realtor/newsroom/realtors-embrace-ai-digital-tools-to-enhance-client-service-nar-survey-finds · gaar.com/blog/article/nar-realtors-embrace-ai-digital-tools-to-enhance-client-service · housingwire.com/articles/nar-2025-technology-survey-realtor-tech-usage-trends
4. IBM and Ponemon Institute, Cost of a Data Breach Report 2025 (600 organizations); shadow AI figures as reported by TechRepublic. ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai · techrepublic.com/article/news-ai-breach-risks-rise-as-governance-lags
5. 22 Tex. Admin. Code §535.2, Broker Responsibility, subsections (a), (e), (g), (h) and (i). law.cornell.edu/regulations/texas/22-Tex-Admin-Code-SS-535-2
6. Microsoft and LinkedIn, 2024 Work Trend Index, announced May 8, 2024 (31,000 people in 31 countries); workload figure as reported by Fox Business; reluctance figure from a published summary of the report. blogs.microsoft.com/blog/2024/05/08/microsoft-and-linkedin-release-the-2024-work-trend-index-on-the-state-of-ai-at-work · foxbusiness.com/technology/employees-using-ai-work-keeping-it-quiet-specific-reason · kendratech.substack.com/p/microsoft-trends-report-on-the-impact
7. OpenAI Help Center, “Data controls in ChatGPT.” help.openai.com/en/articles/7730893-data-controls-in-chatgpt
8. 24 CFR §180.671, Assessing civil penalties for Fair Housing Act cases (eCFR, current). ecfr.gov/current/title-24/subtitle-B/chapter-I/part-180/subpart-F/section-180.671
9. Software AG survey of knowledge workers, as reported by The HR Director. thehrdirector.com/business-news/ai/half-employees-shadow-ai-users
10. TrustedTech survey of 2,001 US and UK employees, as reported by SecurityBrief. securitybrief.news/story/it-telecoms-workers-most-likely-to-use-shadow-ai

This white paper is provided for general information only. It is not legal advice, and it does not create any attorney-client or advisory relationship. Laws, regulations, penalty amounts and agency guidance change; readers should confirm current requirements in their own states and consult qualified counsel about their specific obligations. RAICB™ certification is a point-in-time attestation that governance practices are in place. It is not a guarantee of legal or regulatory compliance, insurance, or a warranty against liability. NIRAP is not affiliated with, endorsed by, or sponsored by NAR, Delta Media Group, IBM, Microsoft, LinkedIn, OpenAI or any other organization named in this paper. REALTOR® is a registered collective membership mark of the National Association of REALTORS®.

© 2026 National Institute for Responsible AI Practice, Corp. This paper may be shared and redistributed in its complete, unaltered form.

AI-assisted  Human-led

How this paper was made

A person at NIRAP initiated this paper, and AI tools helped produce it. After the paper was first published, a person at NIRAP reviewed it, including its facts against their sources. It was reviewed and approved on October 28, 2026.

The label does not guarantee that this paper is free of mistakes or errors. It means a person applied due diligence to verify the output.

If you find an error, email contact@nirap.org. Read how NIRAP uses AI at nirap.org/how-we-use-ai.