AI GOVERNANCE PLAYBOOK

FOR BUSINESS ADVISORS

A Practical Guide to Using AI Responsibly in Your Practice

This playbook includes:

Part 1: Why AI Governance Matters & How to Get Started
Part 2: Your AI Governance Policy Template (fill-in-the-blanks)

Powered by SavvaiEdge

IMPORTANT DISCLAIMER
This playbook and policy template are provided for informational purposes only and do not constitute legal, accounting, or professional advice. We strongly recommend having your customized policy reviewed by an attorney familiar with your practice and jurisdiction before implementation.

PART 1

Why AI Governance Matters

The Opportunity

AI is transforming how business advisors serve their clients. Tools like ChatGPT, Claude, and specialized platforms are helping advisors research faster, analyze deeper, and deliver more value. If you're not using AI yet, you're falling behind. If you are using AI, you're ahead of the curve.

But here are two questions your clients and insurers will eventually ask:

"How do you handle AI? Is my data protected?"

When that moment comes, you want a professional answer—not an awkward pause.

Get Ahead of the Curve

Having an AI governance policy isn't about bureaucracy. It's about:

- **Professional credibility** — Show clients you take their data seriously
- **Competitive differentiation** — Most advisors can't answer the "AI question" well
- **Peace of mind** — Know you're using AI responsibly
- **Future-proofing** — Regulations are coming; be ready before they arrive

This playbook gives you a practical framework and a ready-to-use policy template you can put into practice quickly.

The Two-Tier Model: A Practical Framework

AI governance doesn't have to be complex. There are two main categories of business AI use:

Tier 1: Client Work	Tier 2: Everything Else
Any AI use involving: • Client data • Client deliverables • Client advice	AI use for: • General research • Learning • Internal tasks
Use a governed platform (like SavvaiEdge) that automatically protects client data and provides the infrastructure for a supportable AI governance program. *Any platform with equivalent capabilities—data anonymization, audit trails, human review workflows—can support Tier 1 governance; SavvaiEdge is purpose-built specifically for business advisors.*	Use any AI tool you like—just never input client data

That's the core framework. Tier 1 requires governance infrastructure. Tier 2 requires common sense.

Four Steps to Get Started

You can put AI governance into practice for your firm with four straightforward steps:

Step 1: Customize Your Policy

Use Part 2 of this playbook. Fill in the [brackets] with your firm's information. The template is designed to be straightforward—most advisors complete it in 30–60 minutes.

Step 2: Set Up Your AI Platform

For Tier 1 (client work), you need a platform that provides automatic data anonymization, audit trails, and human review tracking. Your governed AI platform should handle client data protection automatically—removing client names and PII patterns before data reaches AI models—and log every interaction for compliance evidence.

Step 3: Update Your Engagement Process

Add AI disclosure language to your engagement letters (template provided in Part 2). Decide how you'll communicate with existing clients—proactive email, mention at next meeting, or respond when asked.

Step 4: Start Using It

Use your governed platform for client work, review AI outputs before they go to clients, and you're operating with professional AI governance. The goal is a consistent, defensible practice—not perfection on day one.

> **For Multi-Advisor Firms:**
> Add a team training step (30-minute walkthrough of the policy) and collect signed acknowledgment forms. The policy template includes an acknowledgment form in the appendix.

Optional Considerations

Depending on your practice, you may also want to:

- **Have an attorney review your customized policy** — Recommended, especially if you serve clients in regulated industries. A quick review is usually sufficient; you don't need a rewrite.
- **Inform your insurance broker** — Some advisors proactively notify their professional liability carrier. This isn't required, but if your broker asks about AI use, your policy demonstrates responsible practices.
- **Set a calendar reminder for annual review** — AI regulations and best practices are evolving. A regular review keeps your governance current.

What This Policy Enables

With your AI governance policy and supporting infrastructure in place, you can:

- Confidently answer client questions about AI use
- Generate compliance reports showing human review rates and data protection metrics
- Demonstrate professional AI practices to prospects and referral partners
- Meet enterprise client requirements for AI governance documentation

Your Tier 1 platform should provide governance infrastructure aligned with the predominant frameworks for responsible AI and information security, including controls for data protection, auditability, and human oversight.

PART 2

AI Governance Policy Template

> *Note: This template is provided as a starting point and should be adapted to reflect your firm's specific practices and legal requirements.*

[YOUR FIRM NAME]
AI Governance Policy

Policy Owner	[Name and Title]
Effective Date	[Date]
Next Review	[Date + 1 Year]

1. Purpose and Scope

This policy sets out how [Your Firm Name] uses artificial intelligence (AI) in our work with clients. Our goal is to gain the benefits of AI while protecting client confidentiality and maintaining the quality and integrity of our advice.

This policy applies to everyone who works with us—employees, contractors, and partners—whenever they use AI tools in connection with our clients or our firm.

2. Two-Tier Governance Model

We use a two-tier model to govern AI use, based on one key question: is client work involved or not?

Tier 1: Client Work	Tier 2: General Use
Scope: Any AI use involving client data, client deliverables, or client advice	**Scope:** Research, learning, internal documents, personal productivity
Platform: Governed AI platform required (see Section 3.1)	**Platform:** Any AI tool, following guidelines below
Requirements: • Automatic data protection • Full audit trail • Human review before delivery	**Requirements:** • Never input client data • Use good judgment

3. Client Work Requirements (Tier 1)

3.1 Platform Requirement

Whenever AI is used for client information, client deliverables, or client advice, it must be done through our firm's designated Tier 1 AI platform. Team members must not use consumer AI tools (such as ChatGPT, Claude.ai, Gemini, Perplexity, etc.) directly for client work.

Our Tier 1 platform should automatically remove client company names and common PII patterns (such as email addresses, phone numbers, SSNs, and street addresses) before information is sent to AI models. Note that individual people's names are generally not removed automatically — team members should avoid including personal names in AI prompts, and any source documents containing personal names should be reviewed before processing. Team members should also avoid entering highly sensitive unformatted data (such as SSNs or financial account numbers) in free-text fields, as automated detection may not catch every variation. Every AI interaction should be logged with timestamps, user attribution, and which models were used.

3.2 Human Review Requirement

All AI-generated content that will be shared with a client must be reviewed by a human before it goes out.

When you review AI output, you should:

- Read the full response, not just the parts you expect to use
- Check all numbers and calculations against the underlying documents
- Make sure the conclusions and recommendations fit this particular client's situation
- Ask yourself: "Would I be comfortable signing my name to this?"
- Record the review using your platform's review tracking feature and add any necessary notes

> **Important:** AI systems can produce confident, detailed answers that are simply wrong—especially when it comes to numbers, statistics, and calculations. Do not rely on AI-generated figures unless you have verified them.

3.3 Permitted Uses

Examples of appropriate uses of our Tier 1 platform for client work include:

- Researching and analyzing client situations
- Drafting reports, memos, and other client deliverables
- Summarizing documents, meeting notes, and other source materials
- Conducting industry, market, and competitive research
- Generating client-specific strategic recommendations using consulting frameworks
- Receiving proactive client intelligence and recommendations via automated briefings

4. General AI Use (Tier 2)

For AI use that does not involve client data, team members may use any AI tool. This includes general industry research, learning new concepts, drafting internal documents, brainstorming, and personal productivity.

4.1 Universal Prohibitions

Some information must never be entered into any AI tool, under any circumstances. This includes:

- Client names, client company names, or other details that clearly identify a client
- Personal information such as individual names, Social Security numbers, birthdates, or home addresses
- Financial account numbers (for example, bank account details or tax identification numbers)
- Any information covered by a nondisclosure or confidentiality agreement
- Proprietary or confidential information belonging to [Your Firm Name]

If you are unsure whether something is sensitive, we will either run it through our Tier 1 platform (which provides automatic protection) or ask [Policy Owner] before proceeding.

5. Data Protection

When our governed AI platform is used for client work, the following protections should be applied automatically:

- Client company names are replaced with anonymous identifiers before reaching AI models
- PII patterns (emails, phone numbers, SSNs, addresses) are detected and removed
- All anonymization actions are logged with proof for audit purposes
- Client data is never used to train AI models
- All data is encrypted in transit and at rest
- Individual names are not automatically anonymized; team members are responsible for omitting personal names from AI prompts, and administrators should review source documents for personal identifiers before processing

6. Client Disclosure

[Your Firm Name] is transparent about our use of AI tools.

6.1 New Clients

All new engagement letters include disclosure that we use AI-powered tools with appropriate data protection measures. Standard language:

> **Technology and AI Tools:** We use modern technology tools, including AI-powered research and analysis platforms, to improve the quality and efficiency of our services. When we use these tools with your information, we do so within a governed framework that includes automatic data anonymization, detailed audit trails, and documented human review of all deliverables. Your confidential information is protected with strong security controls,

> and your data is not used to train AI models. If you would like more information, we can share documentation describing our AI governance practices.

6.2 Existing Clients

[Describe your approach: "Existing clients will be informed via email" or "at next meeting" or "upon request"]

6.3 Client Inquiries

If a client asks about AI use, respond honestly. Example response:

"Yes, we do use AI tools as part of our research and analysis, much like we use Excel or other data sources. We use them inside a governed platform that automatically protects your confidential information, and we review all AI-assisted work before it is shared with you. If you'd like, I can walk you through our AI governance practices in more detail."

7. Documentation and Compliance

Our AI governance platform maintains complete records of AI usage and compliance status. [Policy Owner] should review the platform's AI Governance Dashboard [weekly/monthly] to monitor human review compliance and data protection metrics.

Compliance reports should be available on request for clients or auditors in standard formats (PDF, Word, CSV, or JSON).

8. If Something Goes Wrong

If something goes wrong—for example, client data is entered into an unapproved AI tool, AI-generated content is sent to a client without review, or a significant AI error reaches a client—take the following steps:

- Notify [Policy Owner] immediately at [email/phone].
- Write down what happened, when it happened, and which clients or matters may be affected.
- Work with [Policy Owner] to decide what remediation is needed, including whether any clients need to be notified.

9. For Multi-Advisor Firms

(Skip this section if you are a solo practitioner)

9.1 Training

All team members must complete policy training before using AI for client work. Annual refresher training is recommended.

9.2 Acknowledgment

All team members must sign the acknowledgment form confirming they have read, understood, and agree to comply with this policy. (See Appendix A.)

9.3 Firm Portal

Our AI governance platform's firm management portal provides centralized governance oversight, aggregate compliance metrics, and firm-wide policy enforcement.

10. Policy Review

This policy should be reviewed annually, when AI regulations change, after any significant incident, or when [Your Firm Name]'s AI tools or practices change materially.

Appendix A: Staff Acknowledgment Form

(For multi-advisor firms only)

AI GOVERNANCE POLICY ACKNOWLEDGMENT

I acknowledge that:

- I have received and read the AI Governance Policy.
- I understand how Tier 1 (Client Work) and Tier 2 (General Use) apply to my work.
- I understand that our designated governed AI platform is required for all AI work involving clients or client information.
- I understand my responsibilities for reviewing AI-generated content before it is shared with clients.
- I agree to follow this policy in my work for [Your Firm Name].

Name (Print):	
Signature:	
Date:	