Contents

AI Acceptable Use Policy for Financial Advisory Firms

Template Version 1.0 Last Updated: March 2026 Provided by AI Secretary

---

Purpose

This AI Acceptable Use Policy establishes guidelines for the appropriate and compliant use of artificial intelligence tools within [FIRM NAME], ensuring alignment with SEC, FINRA, and state regulatory requirements while protecting client information and maintaining operational integrity.

Scope

This policy applies to: - All registered representatives and investment adviser representatives - Administrative staff with access to client information - Third-party contractors and vendors using AI tools on behalf of the firm - All AI-powered tools, platforms, and services used for business purposes

---

Policy Statement

General Principles

1. **Compliance First**: All AI tool usage must comply with existing regulations, including:
    - SEC Regulation S-P (Privacy of Consumer Financial Information)
    - FINRA Rule 3110 (Supervision)
    - State privacy laws (CCPA, VCDPA, etc.)
    - Firm's existing data retention and cybersecurity policies
2. **Client Data Protection**: Client personally identifiable information (PII), account details, and confidential information must be safeguarded at all times when using AI tools.
3. **Fiduciary Duty**: Representatives remain fully responsible for all advice and recommendations, regardless of AI assistance used in preparation.
4. **Transparency**: The firm will maintain transparency with clients regarding the use of AI tools that process their information.

Approved AI Tools

Current Approved Tools

Tool Name	Purpose	Approval Date	Approved For
[AI Secretary]	Meeting notes, CRM updates	[DATE]	All advisors
[Add others]	Purpose	[DATE]	[Roles]

Tool Evaluation Process

Before any AI tool is approved for use:

1. **Vendor Due Diligence** must be completed (see Appendix A)
2. **Security Review** by IT/Compliance officer
3. **Data Handling Assessment** to ensure alignment with retention policies
4. **Written Approval** from Chief Compliance Officer (CCO)

Prohibited Uses

Representatives may NOT:

1. **Input client PII into unapproved AI tools**, including:
    - Consumer AI platforms (ChatGPT, Claude, Gemini, Perplexity, etc.)
    - Free transcription services
    - Unapproved document analysis tools
    - Browser extensions with AI capabilities
2. **Use AI to generate investment advice** without human review and verification
3. **Share client documents** (financial plans, tax returns, account statements) with AI tools unless explicitly approved
4. **Use AI-generated content** in client communications or marketing materials without:
    - Review by a qualified professional
    - Verification of accuracy
    - Compliance approval if required
5. **Bypass compliance review** by attributing decisions or advice to AI tools

---

Acceptable Uses

Representatives MAY use approved AI tools for:

1. **Administrative Tasks**:
    - Meeting note-taking and documentation
    - Calendar management and scheduling
    - Email drafting (non-investment-related)
    - Task management
2. **Research and Analysis** (with human verification):
    - Market research and trend analysis
    - Economic data compilation
    - Industry news summaries
    - Educational content creation
3. **Internal Operations**:
    - Workflow optimization
    - Document organization
    - Training materials development
    - Process documentation

Data Handling Requirements

What Data Can Be Input

Permitted: - Meeting agendas and general discussion topics - General financial planning questions (without client-specific details) - Industry research queries - Public information

Prohibited Without Approval: - Client names, Social Security numbers, account numbers - Personal financial details (income, net worth, account balances) - Health information, estate planning details - Any information that would identify a specific client

Data Retention Alignment

AI tools used by the firm must: - Align with the firm's data retention policy ([X] years for client records) - Provide deletion capabilities and verification - NOT retain data longer than necessary for business purposes - Comply with proper disposal requirements under Reg S-P

Supervision and Monitoring

Representative Responsibilities

1. **Disclose AI Tool Use**: Representatives must disclose any AI tools they wish to use to their supervisor and compliance officer
2. **Annual Attestation**: Sign annual attestation confirming compliance with this policy
3. **Report Violations**: Immediately report any unauthorized AI tool use or data breaches
4. **Review AI Outputs**: Verify accuracy of all AI-generated content before use

Firm Responsibilities

1. **Quarterly Reviews**: Compliance will conduct quarterly reviews of AI tool usage
2. **Spot Checks**: Random audits of meeting notes, communications, and work product
3. **Training**: Annual training on AI risks, acceptable use, and policy updates
4. **Vendor Monitoring**: Annual review of approved AI vendors' security posture and terms of service

---

Training Requirements

All representatives must complete:

1. **Initial Training**: Within 30 days of hire or policy adoption
   - AI risks and regulatory implications
   - How to identify prohibited AI tools
   - Data handling best practices
   - Process for requesting approval of new tools
2. **Annual Refresher Training**: Every 12 months
   - Policy updates
   - Case studies of AI-related compliance failures
   - New approved tools and features
   - Regulatory developments
3. **Attestation**: Sign and date acknowledgment of training completion

---

Consequences of Violations

Violations of this policy may result in:

1. **First Offense**: Written warning, mandatory retraining
2. **Second Offense**: Suspension of AI tool access, formal disciplinary action
3. **Serious Violations** (e.g., inputting client SSNs into ChatGPT):
   - Immediate termination
   - Potential regulatory disclosure
   - Reporting to FINRA/SEC if required

Policy Review and Updates

This policy will be reviewed: - **Annually** at minimum - **As needed** when: - New AI tools are adopted - Regulatory guidance is issued - Material changes to vendor terms of service occur - Incidents or violations occur

---

Appendix A: Vendor Due Diligence Checklist

Use this checklist when evaluating any new AI tool:

Security & Compliance

☐ What security certifications does the vendor hold? (SOC 2, ISO 27001, HITRUST)
☐ When was the last security audit conducted?
☐ Has the vendor experienced any data breaches in the past 3 years?
☐ Does the vendor maintain cyber insurance?

Data Handling

☐ Where is client data stored? (Cloud provider, geographic location)
☐ How long is data retained?
☐ Can data be deleted on demand? Can you verify deletion?
☐ Is data encrypted in transit and at rest?
☐ Does the vendor use customer data to train AI models?

Terms of Service

☐ What happens to data if the vendor is acquired?
☐ What happens if the vendor goes out of business?
☐ Can terms of service be changed unilaterally?
☐ Are there data portability provisions?

Regulatory Alignment

☐ Does the tool comply with Regulation S-P?
☐ Can it support FINRA/SEC recordkeeping requirements?
☐ Does it align with our data retention policy?

☐ Can it fulfill data subject access requests (DSARs)?

Incident Response

☐ What is the vendor's breach notification SLA?
☐ Who is our point of contact for security incidents?
☐ Does the vendor provide incident response support?

Business Continuity

☐ What is the vendor's uptime SLA?
☐ What happens if the service goes down during critical business hours?
☐ Can we export data if we need to switch vendors?

Appendix B: Representative Attestation Form

I, [NAME], acknowledge that:

1. I have read and understand the AI Acceptable Use Policy
2. I have completed required training on AI risks and acceptable use
3. I will only use AI tools that have been approved by the firm
4. I will NOT input client PII into unapproved AI tools
5. I understand that violations may result in disciplinary action, up to and including termination
6. I will report any unauthorized AI tool use I observe
7. I will immediately notify my supervisor if I accidentally input client data into an unapproved tool

Signature: _____ **Date:** _____
Supervisor Signature: _____ **Date:** _____

Appendix C: AI Tool Request Form

Representative Name: _____ **Date:** _____

Tool Information: - Tool Name: _____ **- Vendor:** _____ **- Website:** _____ **- Purpose/Use Case:** _____ **- What client data will it access?** _____

Security Information: - Security certifications: _____ **- Data retention policy:** _____ **- Data storage location:** _____

Business Justification: - Problem this tool solves: _____ **- Alternative solutions considered:** _____ **- Estimated time/cost savings:** _____

Compliance Review: - [ ] Vendor due diligence checklist completed (attach) - [ ] Reviewed vendor privacy policy and terms of service (attach) - [ ] Confirmed tool aligns with firm data retention policy

CCO Approval: - [ ] Approved - [ ] Denied - [ ] Needs additional information

CCO Signature: _____ **Date:** _____
Notes: _____

Contact Information

Questions about this policy? Contact: [COMPLIANCE OFFICER NAME] Email: [EMAIL] Phone: [PHONE]

To request approval of a new AI tool: Submit AI Tool Request Form (Appendix C) to [EMAIL]

To report a violation or incident: Contact: [COMPLIANCE OFFICER] immediately Email: [EMAIL] Phone: [PHONE]

This template is provided for informational purposes only and does not constitute legal or compliance advice. Firms should consult with legal counsel and compliance professionals to ensure policies align with their specific regulatory obligations and business needs.

Template Version 1.0 | March 2026