

AI Governance Policy and Responsible Use Guidelines

A practical policy for safe, ethical, accurate, and effective AI use across 10Fold services and operations

*This framework governs how 10Fold uses AI in delivering services to clients and operating our business.

Document Field	Information
Effective date	July 17, 2026
Review cycle	At least every six months, or sooner if tools, client requirements, laws, risks, or business processes materially change

Our Commitment

AI enhances how we research, analyze and develop communications strategies, but it never replaces expert judgment. Every recommendation delivered by 10Fold is reviewed by experienced professionals, supported by verified evidence and aligned with each client's confidentiality requirements. We use AI to improve quality, efficiency and insight while maintaining the standards of accuracy, transparency and trust our clients expect.

1. Purpose

10Fold encourages the responsible use of approved AI tools to improve productivity, strengthen the quality of work, accelerate research and analysis, and help teams deliver better outcomes for clients and the agency. AI may be used as a thought partner, editor, research assistant, formatting aid, and workflow accelerator. AI must not replace human judgment, professional accountability, client or agency strategy, or required management review.

2. Scope

This policy applies to all 10Fold employees, contractors, and approved partners who use AI tools for client work, 10Fold marketing, sales, recruiting, HR, finance, IT, operations, analytics, automation, or internal communications. It applies to generative AI tools, AI-enabled writing tools, image or video generation tools, transcription and summarization tools, research tools, coding assistants, analytics tools, and workflow automation tools that use AI.

This policy should be read together with applicable 10Fold confidentiality, security, HR, client-service, and information-handling policies. Where a client agreement or manager instruction is stricter than this policy, the stricter requirement applies.

3. Guiding Principles

- **Human accountability:** AI supports our work, but every client deliverable is reviewed, validated and approved by experienced professionals. Human judgment remains central to every recommendation, strategy and communication.
- **Client trust:** AI use must never compromise client confidentiality, strategy, data, intellectual property, or reputation.
- **Accuracy and verification:** AI-generated content must be reviewed by the SME, fact-checked, source-checked, and edited by a human before it is used or shared.
- **Approved tools only:** Team members may use only AI tools approved by 10Fold for the applicable use case and data type.
- **No shadow AI:** Team members may not use unapproved personal AI accounts or public AI tools for client, employee, financial, operational, or confidential 10Fold work.
- **Transparency when required:** AI use should be disclosed when a manager, client, contract, policy, or reasonable business expectation requires disclosure.
- **Risk-based review:** Higher-risk AI use requires stronger safeguards, approval, documentation, and human review. Speak with leadership about specific questions.
- **Responsible marketing:** AI must not be used to generate misleading claims, fake proof points, unsupported statistics, fabricated sources, fake engagement, or deceptive synthetic content.

3a. AI Training and Education

Responsible AI use begins with education. All 10Fold team members receive ongoing training on responsible AI practices, including data protection, confidentiality, prompt engineering, verification, copyright considerations and ethical AI use. Training is regularly updated as AI technologies, regulations and best practices evolve.

4. How AI Helps 10Fold Team Members

AI is expected to help 10Fold teams improve efficiency and quality when used with judgment and care.

- **Speed and productivity:** AI can reduce time spent on repetitive, manual, or first-draft tasks, giving teams more time for strategy, creativity, client counsel, and quality control.
- **Improved quality:** AI can help expand thinking, identify gaps, suggest alternate structures, improve clarity, and test whether a draft is complete, differentiated, and audience appropriate.
- **Better outcomes:** AI can serve as a reviewer, editor, challenger, or role-play partner to improve the strength of recommendations, messaging, content, and client communications.

- **Learning and process support:** AI can help team members understand unfamiliar topics, explore alternate methods, draft checklists, and work through assignments where a process has not yet been fully defined.
- **Understanding 10Fold policies and resources:** AI can help 10Fold staff find information about 10Fold policies using designated resources (such as custom GPTs).
- **Managing time and priorities:** AI can help 10Fold staff prioritize tasks and identify opportunities for growth.

5. Data Classification and AI Input Rules

Before entering information into any AI tool, team members must classify the information and confirm that the tool is approved for that data type and use case.

Data Category	Examples	AI Use Rule
Public information	Published articles, public websites, public analyst reports, public company descriptions, public social posts.	Generally allowed in approved tools. Verify sources and dates before relying on output.
Internal non-sensitive information	Internal notes, general process drafts, non-confidential templates, non-sensitive brainstorming.	Allowed in approved tools when business-appropriate. Review output before use.
Client confidential information	Client strategy, messaging, roadmaps, unreleased announcements, customer lists, media plans, campaign performance, source interviews, client-provided documents.	Use only in private tools approved for confidential client work and only when permitted by client requirements. Manager review required for important deliverables.
Employee, candidate, or HR information	Reviews, compensation, interview notes, recruiting feedback, performance concerns, personnel records.	High risk. Use only with HR-approved processes and tools where data and output remains private. AI must not make or materially determine employment decisions.
Financial or business-sensitive information	Budgets, forecasts, revenue, compensation planning, billing, payroll, bank details, investor or board materials.	Medium to high risk. Use only with Finance-approved private processes and tools. Human validation required.
Legal, regulatory, or contractual information	Contracts, legal claims, compliance questions, litigation, subpoenas, regulatory inquiries, client legal positions.	High risk. Requires approval from leadership and legal counsel as appropriate. AI output is not legal advice. Use only with private tools and data sets.
Security-sensitive information	Passwords, API keys, access tokens, private keys, incident details, vulnerability data, system architecture, privileged access information.	Restricted. Do not enter passwords and pass keys into AI tools unless 10Fold IT/security has specifically approved the use case and tool. Credentials must never be entered.
Regulated or highly sensitive personal data	Government identifiers, health data, precise personal location, financial account data, sensitive demographic data.	Prohibited unless specifically approved by leadership, legal, and IT/security for a documented use case with appropriate safeguards.

- When in doubt, we do not enter the information into AI until the use case, tool, and review process are approved.
- We do not paste passwords, credentials, access tokens, private keys, or security secrets into any AI tool.

- We do not enter client information into an AI tool if the client has prohibited AI use or if the contract limits such use.

6. Approved AI Uses

AI may be used for the following activities when the tool, input data, and review process are appropriate for the level of risk.

6.1 Client and 10Fold Writing Projects

- Expand source questions for subject matter experts.
- Propose or expand an outline based on a drafted pitch or abstract.
- Evaluate the completeness of an outline.
- Identify missing arguments, proof points, or audience considerations.
- Test whether a draft is differentiated from similar published content.
- Edit for clarity, structure, tone, grammar, and flow.
- Simplify sections that are too wordy, technical, or complex.
- Assess whether content may appear overly generic or AI-generated.
- Identify potential sources to support assertions.
- Repurpose approved existing content for another format, audience, or channel.

6.2 Email and Client Communications

- Improve tone, brevity, clarity, and completeness in internal, prospect, and client communications.
- Draft options for difficult or nuanced messages, provided the final message is reviewed and owned by a 10Fold team member.
- Check whether the communication is appropriate for the recipient, relationship, and business context.

6.3 Content Formatting

- Format content into a requested style, structure, template, or channel format.
 - Load 10Fold logos into paid AI versions
 - Add the term “confidential” or “client confidential” to important documents
 - Use correct RPG colors when creating formal documents
- Convert approved content into outlines, checklists, briefs, talking points, or other formats.
- Apply stylistic changes to marketing and sales decks in PowerPoint.

6.4 Excel, Reporting, and Data Analysis

- Build or troubleshoot formulas.
- Improve spreadsheet formatting.
- Create document linkages.
- Summarize and explain analysis of non-sensitive data.

- Suggest ways to display or explain information.

6.5 Sales and Prospect Communications

- Improve sales messaging, objection handling, account research, and prospect communications.
- Use approved selling frameworks, including Same Side Selling principles, to improve clarity and relevance.
- Develop potential media angles based on previous content from SMEs.
- Analyze content from prospects to generate keywords and identify gaps or white space.
- Conduct outreach workflows in approved AI tools with content and cadence pre-approved by humans.
- Acceptable inputs include public company data, approved 10Fold messaging, and client-provided briefs authorized for AI use. Prohibited inputs include unauthorized sensitive prospect PII and confidential internal financial data. All AI-generated prospecting emails must undergo manager review to ensure alignment with 10Fold quality standards and Same Side Selling principles.

6.6 Process Automation

- The IT Manager will define acceptable IT inputs, prohibited data use, review requirements, and whether AI-generated IT documents require executive review before use.
- Automate repetitive workflows across approved business systems after the automation has been reviewed for accuracy, privacy, security, and business impact.
- Prepare internal status updates, schedule recruiting workflows, route draft materials for approval, or generate draft notifications based on defined triggers.
- Require approval before deploying automations that involve client data, employee data, financial information, system access, external communications, or decision-making.
- Finance may use approved AI tools to automate routine tasks such as spreadsheet support, reporting, budgeting, forecasting summaries, reconciliations, and process documentation. All AI-generated outputs must be reviewed and validated by the Director of Finance. AI may not approve transactions, process payroll, authorize payments, submit tax filings, or bypass internal controls and approval processes.

7. Department-Specific AI Requirements

Area	Approved Uses	Requirements and Restrictions
Social, Digital and Marketing Services	Draft social copy based on customized prompts, adapt approved content for channels, develop content calendars, test messaging, summarize public platform trends, support reporting narratives, role play targeting and audience perspectives.	Do not create fake engagement, fake reviews, undisclosed synthetic content where disclosure is required, misleading performance claims, or content that violates client or platform requirements. Image, video, likeness, or voice generation requires rights and approval review.

Area	Approved Uses	Requirements and Restrictions
HR and Employee Reviews	Organize manager notes, improve wording, summarize documented performance themes, make language more objective and constructive.	AI must not make or materially influence hiring, compensation, promotion, discipline, termination, performance ratings, or other employment decisions. HR must review any AI-assisted process that could affect an employee. Do not enter confidential information into any AI platform.
Finance	Support spreadsheet formulas, budget formatting, scenario summaries, variance explanations, and non-sensitive analysis.	Financial analysis involving budgets, compensation, payroll, billing, forecasts, or revenue is medium to high risk. Finance must approve processes and validate outputs before reliance.
IT and Security	Support troubleshooting, scripting, documentation, and workflow automation in approved environments.	Do not enter credentials, access tokens, private keys, incident details, vulnerability information, privileged access data, or sensitive architecture into AI tools without IT/security approval. Human review is required before using AI-generated code or scripts.
Recruiting	Draft/update job descriptions, draft/update reviews, improve outreach & create automated sequences, summarize interview notes, prepare candidate communications, and scheduling assistance.	AI may not be the sole or primary basis for screening, ranking, rejecting, or selecting candidates. Recruiting processes using AI must be reviewed for fairness, consistency, and compliance. Do not enter personal information about candidates.
10Fold Marketing	Draft social posts based on customized prompts, help with outlines or edits to LinkedIn articles and newsletters, adapt approved content for channels, develop content calendars, test messaging, provide research support, support reporting narratives	Do not create fake engagement, fake reviews, undisclosed synthetic content where disclosure is required, misleading performance claims, or content that violates client or platform requirements. Image, video, likeness, or voice generation requires rights and approval review.
Sales	Improve sales messaging, objection handling, account research, research prospects and competitors and prospect communications.	Do not enter credentials in any programs. Only use client-provided briefs in tools authorized for confidential data. Do not enter unauthorized sensitive information. Do not vary from 10Fold messaging and campaigns.

8. Prohibited AI Uses

1. We do not ask AI to create a document on a topic without approved direction, source material, audience context, objective, outline, length, tone, required proof points, and review criteria.
2. We do not enter confidential, regulated, proprietary, employee, customer, financial, legal, security, or sensitive client data into public or unapproved AI tools.
3. We do not use personal AI accounts for client work, 10Fold confidential work, employee matters, financial work, or operational workflows.
4. Finance Prohibited Individuals without approved access to Finance data, users who have not completed required AI and security training, contractors or third parties without authorization, and any employee using unapproved AI platforms for Finance-related activities.
5. We do not deliver AI-generated output to a client or internal stakeholder without appropriate review, fact-checking, and approval.

6. We do not use AI when a client, contract, project requirement, or manager has prohibited AI use.
7. We do not use AI to generate fake quotes, fake reviews, fake testimonials, fake sources, fake media coverage, synthetic engagement, or misleading claims.
8. We do not rely on AI-generated citations, statistics, legal interpretations, financial recommendations, or technical claims without independent verification.
9. We do not use AI to make final decisions about employees, candidates, clients, vendors, budgets, legal matters, security incidents, or other material business outcomes.
10. We do not upload passwords, credentials, access tokens, private keys, sensitive security information, or confidential system documentation into AI tools.
11. We do not use AI-generated images, likenesses, voices, or synthetic media without confirming rights, permissions, disclosure obligations, and client approval.

9. Risk Levels for AI Use

Risk Level	Description	Examples	Required Controls
Low	Uses generally involving public information, non-sensitive drafting, formatting, brainstorming, or learning.	Brainstorming, rewriting internal notes, summarizing public content, finding public sources, expanding outlines, formatting text.	Encouraged. Human review required before use. Verify facts with SME and sources.
Medium	Uses involving company context, client context, sales messaging, operational workflows, non-sensitive business data, or content that may be shared externally.	Drafting client emails, creating proposals or presentations, developing marketing content, summarizing non-sensitive business data, preparing prospect communications.	Use only approved tools. Human review required. Manager or teammate review required for important deliverables. Retain enough documentation to explain AI use if asked.
High	Uses involving sensitive data, regulated information, legal matters, HR decisions, financial recommendations, cybersecurity, proprietary IP, client-confidential information, or material business outcomes.	Employee reviews, candidate screening, compensation planning, legal or compliance analysis, cybersecurity, financial forecasts, client-confidential strategy, external automations.	Prior approval required. Use only approved tools and documented processes. Strong human review and final approval required. Document tool, purpose, data type, reviewer, approver, and disclosure decision.

10. Approved AI Tools and Tool Approval Process

Because 10Fold works with confidential client and agency information, team members may only use AI tools approved by 10Fold for the applicable use case and data type. A tool being paid for does not automatically mean it is approved for all use cases or all data types.

Currently Approved Tool	Approved Use Notes
ChatGPT	For clients that allow AI usage, the risk levels noted above should be considered prior to usage. Typical approved uses include: researching data to support pitch and contributed content development, developing outlines for contributed content, summarizing sourcing call meeting notes, identifying media targets, and researching trends.

Currently Approved Tool	Approved Use Notes
Claude	For clients that allow AI usage, the risk levels noted above should be considered prior to usage. Typical approved uses include: researching data to support pitch and contributed content development, developing outlines for contributed content, summarizing sourcing call meeting notes, identifying media targets, and researching trends.
Same Side Selling Coach	Approved for sales messaging, prospect-response strategy, and Same Side Selling guidance. Ensure use of client-provided briefs complies with Section 5 data classification guidelines for confidential information
Buzz AI	Approved for sales and recruitment outreach workflows.
Meltwater	Approved for media and social media monitoring, reporter identification, and outreach.
Perceptra	Approved for classification of articles included in competitive SOVs for clients. E.g., Feature vs. Briefs, Business vs. Trade, etc.
Copilot	Approved for Admin, Finance, HR

New AI tools, AI-enabled features, browser extensions, plug-ins, integrations, or automation tools must be reviewed before use for 10Fold or client-related work.

Approval Criterion	Questions to Answer Before Approval
Business purpose	What problem does the tool solve, and who will use it?
Data use	What data will be entered, uploaded, processed, stored, or generated?
Training and retention	Can vendor staff access the data? Is data used to train models? How long is data retained?
Security	Does the tool support appropriate access controls, account management, encryption, and auditability?
Client restrictions	Do client contracts, scopes, or instructions limit use of AI or third-party tools?
Legal and compliance	Are there privacy, employment, IP, copyright, regulatory, or disclosure issues?
Output risk	Could the output affect employees, candidates, clients, legal matters, finances, security, or reputation?
Owner and monitoring	Who owns the tool internally, and how will use be reviewed over time?

11. AI Review Process

Before using AI for medium or high-risk work, team members should begin with a prescriptive prompt that includes the following:

- The objective of the assignment.
- The audience.
- The approved outline, key messages, or required concepts.
- Any approved source material, QA data, or documentation.
- Source types the AI may use.
- Questions the AI should answer.
- The role the AI should play, such as editor, client, reporter, buyer, analyst, or reviewer.
- Required format.
- Desired length.
- Timeframe for research or source review.
- Any restrictions, such as do not invent sources, use only provided material, or flag uncertainty.

- Prompting the model to ask questions to clarify the task is recommended for improved outcomes.

After receiving AI output, team members must review it for the following:

- Accuracy.
- Completeness.
- Differentiation.
- Tone and brand fit.
- Client fit.
- Source quality.
- Confidentiality concerns.
- Unsupported claims.
- Missing context.
- Overly generic or AI-sounding language.

For all content to be submitted to a publication or client blog, staff should utilize 10Fold's AI QA processes to ensure that the content is not plagiarized or too similar to existing content.

Recommended review questions include:

- Is this accurate?
- Is this differentiated from similar articles, documents, or processes?
- What is missing?
- What assumptions did the AI make?
- What claims require verification?
- What sources support the most important assertions?
- What could be misunderstood by a client, reporter, prospect, employee, or other stakeholder?
- What would make this stronger?

12. Disclosure Requirements

Team members should disclose AI use when a client asks whether or how AI was used, a contract or project requirement requires disclosure, AI materially contributed to a deliverable or recommendation, disclosure is necessary to maintain trust, or a manager asks for the AI process used to create or improve the work. Disclosure does not need to include every minor AI-assisted edit, but it should be clear and accurate when transparency matters.

13. Documentation Requirements

Not every low-risk AI interaction needs to be documented. Medium and high-risk work should be documented at a level that allows 10Fold to explain the tool used, purpose, data entered, human review, final approval, and disclosure decision.

Use Type	Minimum Documentation
Low risk	No formal log required unless requested by a manager or client. Team members remain responsible for accuracy.
Medium risk	Document tool used, business purpose, type of information entered, reviewer, and whether the output was used in a client-facing or external deliverable.
High risk	Document tool used, business purpose, data category, approvals, reviewer, final approver, output use, disclosure decision, and any restrictions or safeguards. Add to the AI Use Log for High Risk.

14. Accuracy, Source, and Quality Control

- AI output must be treated as a draft, not a final source of truth.
- Team members must verify statistics, quotes, citations, URLs, technical claims, legal claims, financial claims, and competitive claims before use.
- AI-generated sources must be checked directly. If a source's accuracy or credibility cannot be verified, it should not be used. Note: technical links can be found through queries with the LLM. Check those links for credibility.
- Client claims, product claims, performance claims, and competitive claims must be supported by evidence by credible (tier 1 or 2) third-party source – including media, analysts, or influencers or partners.
- AI-generated drafts should be edited for accuracy, specificity, voice, and client relevance before use. They should all be compared to the Q&A for the company, division and spokesperson before submitting.

15. Marketing, PR, and Synthetic Content Controls

- We do not use AI to create misleading product claims, inflated performance claims, unsubstantiated market leadership claims, or deceptive AI-related claims.
- We do not create or use fake testimonials, fake customer quotes, fake reviews, fake case studies, fake survey data, fake analyst commentary, or fake media coverage.
- We do not use AI-generated images, video, audio, likenesses, or voices in client or 10Fold materials without confirming rights, permissions, disclosure obligations, and approval.
- We do not use AI to simulate public support, social engagement, reviews, comments, or community activity.
- AI can support content development, but the final message must reflect approved strategy, verified proof points, and appropriate disclosure decisions.

16. AI Governance

10Fold maintains a cross-functional AI governance program responsible for evaluating AI tools, reviewing high-risk use cases, updating governance policies and ensuring AI practices remain aligned with client expectations, security requirements and evolving regulations.

17. Questions, Exceptions, and Escalation

Questions regarding this framework or 10Fold's AI practices may be directed to our leadership team. Governance questions are reviewed through our established AI governance process.

Appendix A: Prompt Checklist

- Objective: What do I want AI to help accomplish?
- Audience: Who is this for?
- Inputs: What approved materials should AI use?
- Boundaries: What should AI not use or assume?
- Role: What perspective should AI take?
- Output: What format, length, tone, and structure do I need?
- Timeframe: What date range should AI consider for research or source review?
- Verification: What claims, sources, or assumptions need checking?
- Confidentiality: Am I allowed to enter this information into this tool?

Appendix B: Reference Sources Used to Inform this Policy

This policy was drafted as a practical internal governance document and 10Fold has reviewed this document with legal counsel.

Sources used to develop this document:

- **NIST AI RMF Resource Center:** <https://airc.nist.gov/airmf-resources/airmf/>
- **ISO/IEC 42001:2023 AI Management Systems:** <https://www.iso.org/standard/42001>
- **FTC guidance on AI privacy and confidentiality commitments:**
<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments>
- **FTC Operation AI Comply press release on deceptive AI claims and schemes:**
<https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>
- **EEOC resource on AI and employment discrimination:**
https://www.eeoc.gov/sites/default/files/2024-04/20240429_What%20is%20the%20EEOCs%20role%20in%20AI.pdf