

Using GenAI Safely

A How-to Guide
for Accounting Firms

Brought to you by



JASON STAATS
Content Creator, Founder

Introduction

Whether you are already familiar with Generative AI tools like ChatGPT, Google Gemini, or Microsoft Copilot, or beginning to explore how such tools can help you boost productivity and build efficiency at your accounting firm, you may have concerns that are holding you back. You want to use these tools safely and responsibly, but don't know how, and don't have the time to figure it out.

You may be thinking...

This technology is fundamentally different than anything else we use. We don't know how to explain its capabilities and use-cases to our staff, or educate ourselves on the risks and best-practices regarding data security and privacy.

You're not alone. In the 2024 Rightworks Firm Technology survey of tax and bookkeeping firms nationwide, nearly 60% of respondents were slow adopters of new technologies like Gen AI. The same Rightworks study also showed firms that *did* adopt new technologies reported as much as 39% more revenue per employee.

Further, a study conducted by OpenAI and the University of Pennsylvania found that accountants have a 100% exposure to GPT-powered software, where exposure is defined as driving a material reduction of time it takes to complete a task. Generative AI tools can help accountants work more effectively and efficiently with fewer people.

Don't let your fear keep you from embracing the enormous value of these tools!

This guide offers up a **practical** advice on how to deploy generative AI technology in a way that is easy, effective, helps improve client offerings and mitigates risks.

Safe AI Use Checklist:

	Designate an AI Champion
	Understand the Benefits
	Understand the Risks
	Select the Right Tools for your Firm
	Determine what types of data are permitted
	Develop an AI Policy
	Ongoing Communications and Training

Section 1

Designate an AI Champion

The primary role and responsibility of the AI champion is the understanding and implementation of AI tools in a responsible manner across your firm. The champion will participate in all of the subsequent steps.

The perfect person for this role is someone who meets most, if not all, of the following criteria:



Holds a deep understanding of your firm - the operations and the people



Has interest in generative AI tools, and an appreciation for the benefits these tools provide



Has the respect of peers and colleagues



Can manage change throughout the organization



Can inspire and excite others towards achieving a goal

Depending on your firm size, you may want to designate more than one champion, or even a small working group. An AI Champion or working group can help build a culture that educates on clear and appropriate guardrails while reinforcing the benefits of GenAI tools and empowering employees to capture the value and improve their work.

Section 2

Understand the Benefits

One of the most important steps to take as your firm is looking to embrace AI tools is a simple one- ask, **“how will this technology benefit this firm?”**



Boost Productivity

Summarize client meetings, get action items from internal meetings, and draft communications such as emails in a fraction of the time it would normally take you to complete those tasks. Productivity gains can free you up to focus on higher-value business tasks.



Augment your Staff

Through creating specialized virtual assistants, you can build the expertise on your team that you need. For example, you can create legal or HR virtual assistants. With GenAI, you can empower your team members to automate tasks, enhancing work satisfaction.



Conduct Research

From quick answers to questions from conversational chat, to industry-specific needs, such as looking up the latest tax codes, GenAI is a fast and powerful way to search vast amounts of information to get you relevant answers.

It's still early days for using Generative AI at firms and businesses. As you start to use Generative AI and as tools evolve, you'll find more ways for it to benefit your specific firm, and ready your firm for the future.

Section 3

Understand the Risks

Use of any tool or technology carries with it some amount of risk. GenAI tools are no different. And just like when you deploy any new system, technology or tool, it is important for you to understand how it works, and how to use it safely. Some of the risks involved in using these technologies are:



Confidentiality and Privacy

Sharing confidential information with a GenAI tool can create similar risks as to sharing such information with any third party. In particular, when you submit information into a prompt on a GenAI platform, the platform may retain rights to use that information or publish the output. There is a risk that information shared will become part of a training set for the language model and will therefore be able to be accessed by users of the same tool at other companies. This may be at odds with confidentiality requirements in your client contracts.



Inaccuracy

While Generative AI outputs can be extraordinarily helpful and accurate, the tools are far from perfect. Outputs may contain errors, be misleading, biased, or trained on data that is inaccurate. “Hallucinations” may occur where the Generative AI tool creates information and presents it as a fact.



Ownership of Outputs

You may not effectively own the results / outputs of prompts you input into an AI platform. While there are a number of pending lawsuits in this area, you may not be able to stop others from copying or reusing outputs resulting from your inputs, or stop the GenAI platform from disclosing identical outputs.

We think the biggest blockers to accounting firms is to not breach any ethical or contractual duties to clients with respect to their privacy and confidentiality of data. So how do you get the value out of GenAI tools while keeping your clients' data secure, while avoiding legal liability and reputational damage to your firm?

Section 4

Select the Right Tools

What GenAI tools are permitted at your firm? Best practice is to have at least an initial list of firm-sanctioned tools. Some firms may want to restrict business use of non-sanctioned tools, while others may just request employees that use other tools to notify the AI champion so that the firm can prepare a catalogue of all Generative AI platforms in use.

How do you best review GenAI tools to determine what is right for your firm? Think of an AI developer as any other vendor that you'd want to evaluate from a value and security perspective. Review the provider's terms of use and public statements regarding data, security and associated practices. Your use of any Generative AI tool will be subject to an agreement with the provider of the tool (if there are no terms from a provider, that's a red flag to avoid!).

— **Review the Terms of Use. In particular, seek answers to these questions:**



What are the sources of training data for the tool?



Who at the AI developer can view information input by a user, and can data be shared with anyone else?



Can inputs be used to train the model, or accessed by other users of the model?



Are there restrictions on use?



Are there confidentiality protections of data input?



As a [Firm Name] employee, you are charged with the responsible and appropriate use of the generative AI tools that have been made available to you.

We must only use GenAI Platforms in ways that are lawful, transparent, and fair.

- **Ensure you use business/enterprise version of tools** (i.e., avoid free versions).

Enterprise terms of use should provide greater protections for your firm around confidentiality of inputs and the rights to use prompts and outputs, warranties and other legal protections.

- **Make sure you have implemented any available and appropriate opt-outs related to rights to use prompts and outputs.**

For example, ChatGPT has an opt-out for a user's inputs training the LLM for its Personal plans.

(<https://privacy.openai.com/policies?modal=take-control>).

Section 5

Determine what data you are comfortable authorizing for input

What are the different types of data at play? Here is a way you can think about this:

1

Public Data

This information is available to the public, for example contents of a Wikipedia article.

2

Non-Confidential Data

In addition to public information, this can be non-public information that does not require special protection. It could include information you receive from a client that is not considered confidential or sensitive, or subject to access controls. Non-confidential data should not contain any sensitive information or any personally identifiable information. For example, general business data and anonymized data would be non-confidential. If you redact confidential information out of a data set, the remaining data may be non-confidential.

3

Confidential Information

This is client information that is covered by contractual confidentiality restrictions or information licensed from a third party.

4

Personal Information

This includes information such as names, addresses, phone numbers, SSNs.

Here is a suggestion for how to categorize these data types with available GenAI tools. You should assess this based on your own risk tolerance, and include in your firm’s AI Policy (see Section 5).

Type of Data	Risk Level	Tools Available for Use
Public Data	Low	Generally safe to use in any Generative AI tools
Non-Confidential Data	Low	Generally safe to use in any Generative AI tools
Confidential Information	Moderate	Only firm-sanctioned tools that have data protections
Personal Information (PII)	High	Only firm-sanction tools that have data protections (e.g., no data training.)

Section 6

Develop an AI Policy that captures all of the “rules of the road” for your firm

Develop a clear policy around use of Generative AI tools, that answers important questions:



What tools are OK to use for business purposes?



What company information is OK to input?



What type of review/quality control is required of output?



What use cases are OK?



Where should employees go for help?



Which types of data can be used with which apps?

Section 7

Ongoing Communications & Training

Whether you choose to set aside specific meeting time or try to do your rollout in a more asynchronous manner, we recommend covering the following items:

— Introduce AI Champion and council



Briefly describe the work these individuals have performed and the roles they will assume moving forward.



This is a good time to energize and excite the rest of the firm about the future of AI within the firm and highlight the investment and commitment the firm is making to explore and understand the technology.

— AI policy overview



It is important to properly share the AI policy and any other firm guidelines on AI tools with your internal staff and provide appropriate training.



Allow space for conversation and questions. Some items may be new concepts that require explanation.

— Highlight best practices



Understand the importance of personal responsibility when engaging AI.



Validate and verify important information before sharing with clients or others.



Be aware of submitting sensitive data to AI tools.

— AI training



Educate to key features and functionality of AI products and tools.

In addition, consider working with all of your employees on building a catalogue of AI Tools and Use Cases. Encourage individuals to share examples of positive and negative experiences with this technology. In particular, there should be a place to capture and share out worthwhile use cases that could benefit other employees.

Section 8

FAQs

Here are some sample FAQs that you may receive from your employees or clients, and some suggested responses

Q *What happens if an employee accidentally puts a customer SSN into a free version ChatGPT (without an opt-out on model training)?*

A At the time of this writing, because the user is using a personal plan, the prompt is trained into the model. While a firm should prohibit SSNs from being input into GenAI prompts, it may happen inadvertently.

- ChatGPT has some safeguards in place -- all prompts are stripped of personally identifying info or anything deemed to be sensitive - so what goes into the model likely won't include those details
- Most reputable tools will have implemented measures to prevent the sharing or exposure of sensitive user inputs. However, if the tool you used does not have these measures, or the tool is not properly secured or has vulnerabilities, you should take steps to address the situation. You can reach out to the developer or support team of the tool you used to explain the situation about the information that was accidentally input.

Q *What if I have a vendor or contractor that is using AI tools?*

A If you share confidential information with a vendor or contractor that is using a generative AI tool for work, then many of the same risks would apply. In order to address this, your firm should determine how the vendor is using a generative AI tool for its work for the firm, who is reviewing the output, and what tools are being used.

Example

AI Policy Template

****NOTE:** The following is a draft policy for use of generative AI tools that may not be appropriate for all companies or may require updates to suit a company's particular circumstances. Modify and adapt this to meet your firm's legal, security and operational needs before implementing**

Policy on Generative AI Platforms for [Firm Name]

Introduction and Purpose

This policy governs the use of generative artificial intelligence tools or platforms ("GenAI") by any person in the performance of services for or on behalf of [Firm Name].

Any questions about this policy should be directed to [Insert name and contact details].

A What is Generative AI?








Generative artificial intelligence refers to artificial intelligence technology that creates new content (such as text, audio, data, images, video) ("Output") by leveraging content that the technology was trained on (e.g., through machine learning) ("Training Data") in response to prompts submitted by a user ("Prompts").

The following are examples of Generative AI platforms ("GenAI Platforms"): [Note this chart can be modified, as desired.]

Type of Generative AI	Examples
Text-to-text	Chat-GPT, Copilot, Bard
Text-to-images	DALL-E 2, Stable Diffusion, Midjourney
Text-to-source code	Chat-GPT, GitHub CoPilot, Open AI Codex
Text-to-video	Synthesia, Runway
Text-to-sound	Amper
Text-to-voice	UberDuck

Appropriate Use

Some appropriate business uses for Generative AI include:

-  Sparking creativity
-  Research
-  Automating or assisting with repetitive tasks
-  Generating content for social media and marketing
-  Rapid messaging and correspondence
-  Summarizing meetings or conversations
-  Generating product and business ideas or strategies

B **Generative AI Tool Selection**

Generative artificial intelligence refers to artificial intelligence technology that creates new content (such as text, audio, data, images, video) (“Output”) by leveraging content that the technology was trained on (e.g., through machine learning) (“Training Data”) in response to prompts submitted by a user (“Prompts”).

The following are examples of Generative AI platforms (“Gen AI Platforms”): [Note this chart can be modified, as desired.]

Option 1: [Note: If your firm will only be permitted to use certain platforms:]

Until we, as an organization, better understand the capabilities and risks of the various emerging and generally available AI tools and products, we ask that you limit your work-related interactions with Gen AI Platforms to those tools listed below.

List of Approved Apps by Data Types

Type of Data	Approved Apps	Examples
Public Data		
Non-Confidential Data		
Confidential Information		
Personal Information (PII)		

— *Note: If you have generative AI needs that are not being met by these provided tools, please contact <insert person and method here> to discuss options and alternatives. Your specialized, unmet use case may provide an opportunity to participate in early-release, beta, pilot, or as-needed software trials.*

Option 2:

Employees are encouraged to explore and experiment with generative AI tools for professional development, research and other business purposes. The firm recommends that employees use a Gen AI Platform listed below. If you would like to use a different GenAI Platform for business purposes, please notify [insert person and method here].


List of Approved Apps by Data Types


Type of Data	Approved Apps	Examples
Public Data		
Non-Confidential Data		
Confidential Information		
Personal Information (PII)		

C

Policy Enforcement

This policy is not optional.

- 

The Company takes use of Generative AI seriously and has developed a multidisciplinary team to be responsible for governance and oversight of the AI policy. If you are unclear how to proceed in a particular scenario, please reach out to [insert name].
- 

Failure to comply with this policy could result in disciplinary action, up to and including termination. If you become aware of any potential violations, please report these to [insert name].

D General Guidance

As a [Firm Name] employee, you are charged with the responsible and appropriate use of the generative AI tools that have been made available to you.

We must only use GenAI Platforms in ways that are lawful, transparent, and fair.

Permitted Behavior

GenAI Platforms may be used in a manner that is not restricted or prohibited by this Policy, such as:



a starting point for ideas or inspiration



a replacement for a search engine and for information gathering



a way to summarize or analyze non-confidential information



[Insert any other permitted use cases.]

Permitted Behavior

The following activities are permitted as long as you both (A) do not engage in any Prohibited Behaviors described above, and (B) do engage in all Required Behaviors described below:

- 1 **YOU MAY** use Generative AI Platforms as a starting point for ideas or inspiration.
- 2 **YOU MAY** use Generative AI Platforms as a replacement for a search engine, and for information gathering.
- 3 **YOU MAY** use Generative AI Platforms for summarizing or analyzing non-sensitive content (such as news articles).
- 4 **YOU MAY** use Generative AI for other use cases which are not prohibited by this policy or any of our other policies.

Prohibited Behavior

The following uses of GenAI Platforms are prohibited:

- 1 **DO NOT** use Prompts or Outputs that are harmful, inappropriate, or violate the Company's standards and policies concerning appropriate workplace conduct.
- 2 **DO NOT** use Outputs for any fact-based use cases where accuracy is important, without additional verification.
- 3 List any uses that your company would like to restrict. This list will vary by company. Include diverse perspectives in an internal discussion about your standards and risk tolerance. Example use cases could (but don't have to) include: performance evaluations, legal contracts, specific report analysis, etc.]

Required Behavior

Any employee that uses a GenAI Platform for business purposes must adhere to the following requirements:

Accuracy

- 1 **DO** review any Output to identify errors, security vulnerabilities, plagiarism and other infringement risks, and other issues.

Records

- 2 **DO** keep records of Outputs that are intended for external use cases.
- 3 **DO** keep records of any GenAI Platforms you use for business purposes.

Transparency

- 4 **DO NOT** hide from, or mislead, any third party regarding the use of artificial intelligence in any Outputs, particularly to the extent the Outputs involve automated decision-making or suggestions.
- 5 If using GenAI Platforms in work for a client **ALWAYS** confirm that such uses are permitted under the client relationship.

GenAI Platform Guidelines

- 6 **DO** comply with any usage policies and other terms of the applicable GenAI Platform. For questions on any such policies, please contact [\[insert name\]](#).

Decision Making

[Firm Name] employs artificial intelligence technology in the creation and development of content and other materials. We are committed to transparent and responsible use, following stringent guidelines to ensure the proper utilization of AI tools. These guidelines are designed to protect against bias, ensure data security and mandate ethical use. In our firm, AI is used to assist not to replace or fully automate our processes. All deliverables are reviewed by individuals who understand our clients, their needs and the limitations of artificial intelligence.

The raw output of generative AI tools must never be used as a deciding factor in the making of decisions which may have material or legal effects upon natural persons, including [Firm Name] employees or clients.

The raw output of generative AI tools must never be used as a deciding factor in the making of decisions which may have material or legal effects upon the [Firm Name] organization.

Ready to take the next step?

Use Spark to create your AI policy in minutes

Build your own AI policy with Spark. Start with our template that applies all the best practices from this guide, and use Spark's conversational Generative AI chat to easily customize it for your accounting firm or business.

Visit ai.rightworks.com to get started for free today.