



PJ Networks AI Safety Guidelines for the Workplace

Purpose

Artificial intelligence can save time, improve productivity, and help businesses move faster. However, it can also expose sensitive information, create security risks, or take harmful actions if it is used without the right safeguards. These guidelines are designed to help small and midsize businesses use AI responsibly while keeping people in control of important business decisions and systems.

Who This Applies To

These guidelines apply to anyone who evaluates, purchases, or uses AI at work, including owners, managers, and employees. This includes AI chatbots, assistants, agents, automations, and AI features built into existing software, especially when they are connected to company systems or data.

Five AI Safety Rules

1. Treat AI Like a New Employee

When an AI tool is given access to company information, treat it the same way you would treat a new employee. **Before enabling any AI tool, confirm what data it can access, what systems it can connect to, and what actions it can take.** Then decide whether it actually needs that level of access.

Many AI tools use the same permissions as the person signed in to them. This means that if a user can open sensitive files, mailboxes, or applications, the AI may be able to access them as well. However, this is not true of every tool. Some AI tools have their own separate access or use company-wide connections that can reach more data than any single user. **For any new or unfamiliar AI tool, always verify how access works before connecting it to business systems.**

Do	Don't
Review with IT what the AI can see, access, and do before it is enabled, including how its permissions work.	Assume the AI only uses your permissions, only sees what you point it to, or is safe with its default settings .
Grant only the minimum data and system access the tool needs, and review access again as its use expands.	Give AI broad access "just in case" it might be useful later.

2. Never Connect AI to Company Data Without IT Involvement

Connecting AI to business systems often looks simple, but a single connection can expose large amounts of company data. **Always consult PJ Networks before connecting AI to business systems**, including Microsoft 365, Google Workspace, SharePoint, Teams, OneDrive, CRM systems, accounting software, shared drives, and other business applications.

IT review needs to happen before the connection is made, not after. Once a tool is connected, it may already have access to company data or systems. Reviewing it first allows IT to confirm what the tool can access, how it stores and shares data, what it can do automatically, and whether it meets any compliance requirements.

Do	Don't
Involve IT before signing in to, purchasing, or connecting any new AI tool.	Move forward just because the setup looks simple or the vendor says the tool is secure.
Confirm who will manage and oversee the tool, and how access can be removed if needed.	Assume a tool is safe because nothing seems wrong. Risks are not always obvious, so check with IT when in doubt.

3. Only Use Business-Grade AI That Has Been Properly Set Up

Anything entered into a free AI tool should be treated as public. **Anything entered into a paid AI tool should also be treated as public until IT has verified that it is configured correctly.** By default, some paid AI services still share your data, keep it, or use it to train their AI unless specific settings are turned off.

A consumer grade paid account alone is not enough. **Use business AI accounts that are owned and administered by the company**, rather than personal accounts, so that settings can be managed, activity can be monitored, and access can be removed when someone leaves. Until a tool is approved, do not enter client information, contracts, financial records, HR data, passwords, confidential business plans, or other sensitive documents into it.

Simple test: If you would not be comfortable seeing the information made public, do not enter it into an AI tool until the tool has been reviewed and approved.

Employees often start using AI tools on their own to save time, sometimes with free or personal accounts. Even with good intentions, this can put company or client information into tools no one has reviewed. **Make sure you know which AI tools are being used in your business, including AI features built into software you already use.**

An AI acceptable use policy makes expectations clear for everyone by spelling out which AI tools are approved, what information can be entered into them, and who to ask before trying something new. It can be a standalone policy or part of your existing acceptable use policy. **If you do not have one yet, PJ Networks can help you draft one that fits your business.**

Do	Don't
Use approved, company-administered AI tools with privacy settings verified by IT.	Use personal AI accounts, free or paid , for company or client data.
Ask IT to confirm how the tool stores, shares, and uses your data , and that the company can manage the account, before anyone uses it.	Assume a paid subscription protects company data by default , or that it can be secured later.
Know which AI tools your team uses , and set clear expectations with an AI acceptable use policy.	Assume employees are only using approved tools without checking or giving guidance.

4. AI Can Help Make Decisions. It Should Not Make Them Alone.

AI can sound confident while still being wrong. Even as AI models become more capable, they can still misunderstand instructions, take steps in the wrong order, overwrite important work, change or delete the wrong information, or act without full context. **Always have a person review AI-generated work before it is used for financial, legal, HR, security, customer-facing, or strategic business decisions.**

Use AI as an assistant, not an authority. AI can research, draft, summarize, organize, and make recommendations, but people should stay in the driver's seat. **A person, not the AI, must always be responsible for the final decision, approval, and action.**

Do	Don't
Check important AI output for accuracy and completeness before relying on it.	Assume an answer is correct because it sounds polished or confident .
Keep a specific person accountable for every approval, decision, and final action.	Let AI make legal, financial, HR, security, or customer-facing decisions on its own .

5. Start Small and Expand Carefully

The safest AI projects are simple, narrow in scope, and read-only, meaning the AI can view information but cannot change it. Good starting points include meeting summaries, email drafts, document search, internal knowledge lookup, task tracking, and research.

Before allowing AI to change data, send messages, approve transactions, or make changes across multiple systems, make sure the right controls are in place. This means someone is clearly responsible for the tool, its access is limited, its activity is monitored, and changes can be undone if something goes wrong.

Do	Don't
Start with low-risk, read-only uses , and review with IT before expanding.	Start by giving AI permission to change records, approve transactions, or send messages .
Add automation only after someone is responsible for it, access is limited, activity is monitored, and there is a way to undo changes.	Allow AI to make changes across systems just because the workflow seems straightforward.

Quick Approval Checklist

- Has the AI tool been reviewed and approved by IT?
- Have we worked with IT to create an AI acceptable use policy, and does this tool fit within it?
- Do we know what data and systems it can access?
- Have we verified how the tool gets its access, such as through the signed-in user's account or a separate company-wide connection?
- Do we know whether our data may be stored, shared, or used to train AI models?
- Is it a business account owned and administered by the company, rather than a personal account?
- Is access limited to only what the tool needs?
- Is a specific person responsible for reviewing important output before action is taken?
- Can the tool change data, send messages, or take actions on its own? If so, has that been specifically approved?

Where to Start

If you want to start exploring AI, **we recommend beginning with the Copilot tools built into Microsoft 365**. Copilot works inside your existing Microsoft 365 environment, so it is tied to your company accounts, works within the permissions your users already have, and does not use your business data to train its AI models. That makes it a practical, lower-risk place to try tasks like summarizing meetings, drafting emails, and finding information across your files.

Many Copilot features are already available at no additional cost with your existing Microsoft 365 business license, so you can start experimenting right away. **If you want to go further, reach out to PJ Networks and we can set you up with a full Microsoft 365 Copilot license.**

To learn more on your own, Microsoft offers free training: [Draft, analyze, and present with Microsoft Copilot](#).

If your business uses Google Workspace instead, **we recommend starting with the Gemini tools built into Workspace**. Like Copilot, Gemini works with your company accounts, only uses content each user already has permission to view, and does not use your business data to train its AI models. To learn more, see Google's guide: [Google Workspace with Gemini](#).

Bottom Line

The biggest AI risk is not the technology itself. It is giving AI access to data, systems, or authority that no one fully evaluated first. AI should help people work more effectively, not replace their judgment or accountability. **Before adopting any AI tool, involve IT, use company-administered accounts, protect confidential data, limit permissions, verify important output, keep people responsible for decisions, and expand gradually.**

AI is changing quickly, and it is not always clear which tools are safe or where to begin. That's where we come in. Whether you are exploring AI for the first time, want to confirm that the tools you already use are set up correctly, or need help planning your next step, we can help you find the right approach for your business. **Contact PJ Networks at support@pj-networks.com with any questions about AI.**