AI Chatbot Use Guidelines

Provided by AXICOM — Jake Nonnemaker

Why This Matters

AI chatbots like ChatGPT, Microsoft Copilot, Google Gemini, Claude, and Perplexity are powerful productivity tools. But how your team uses them — and what data they upload — has real privacy, regulatory, and legal implications. These guidelines are intended to help your staff get the benefits of AI without exposing the firm to unnecessary risk.

What NOT to Upload to Free/Consumer AI Chatbots

Treat free and consumer-tier AI tools as public. Unless you are using an approved enterprise account with a written data-protection commitment, do not upload, paste, or describe any of the following:

- **Personally identifiable information (PII)** — names, addresses, SSNs, birthdates, or contact details of employees, vendors, tenants, or investors.
- **Financial records** — account numbers, statements, tax documents, or banking details.
- **Confidential business documents** — contracts, leases, NDAs, partnership terms, or anything marked confidential.
- **Proprietary or trade-secret information** — strategy documents, pricing models, deal pipelines, or internal processes.
- **Regulated data** — anything covered by HIPAA, GDPR, CCPA, or PCI.

Legal and Regulatory Exposure

Uploading sensitive data to a consumer AI tool can create three categories of risk:

- **Privacy law violations:** GDPR, CCPA, and HIPAA require that personal data be handled securely and shared only with authorized parties. Most free chatbots do not meet these standards.
- **Confidentiality and NDA breaches:** Pasting NDA-covered material into a chatbot can be considered disclosure — even if no human reads it.
- **Loss of trade-secret protection:** Trade secrets are only legally protected if you take reasonable steps to keep them confidential. Uploading them to a third-party AI tool can void that protection.

Free vs. Paid / Enterprise Tiers

The single biggest factor in chatbot privacy is which tier you are using:

Tool	Free / Consumer Tier	Paid / Enterprise Tier
ChatGPT (OpenAI)	Conversations may be used to train future models.	Enterprise: data isolation, no training on your data, no retention.

Tool	Free / Consumer Tier	Paid / Enterprise Tier
Microsoft Copilot	Free Bing/Edge integration may use input to improve services.	Microsoft 365 Copilot: commercial data protection — data is not used for training.
Google Gemini	Data may be used to improve Google services unless you opt out.	Gemini Advanced: more controls, but settings still need configuration.
Claude (Anthropic)	Conversations may be used to improve the model unless you opt out.	Claude Pro / API with data agreements: stronger privacy controls.
Perplexity	Queries may be used to improve search and AI features.	Pro: better controls, but not fully isolated outside enterprise tier.

Bottom line: when handling business data, use a paid or enterprise account with a clear data-protection agreement.

Recommended Practices

- **Use approved enterprise tools first.** Microsoft Copilot Chat inside your Microsoft 365 environment provides commercial data protection by default and should be the first choice for business tasks.
- **Disable chat history and training on consumer tools.** If a consumer chatbot must be used, turn off "Chat History & Training" (or the equivalent) and use incognito modes when available.
- **Redact before you upload.** Strip names, account numbers, and identifying details before asking a chatbot to summarize or analyze a document.
- **Never paste regulated data into a free chatbot.** HIPAA, PCI, and similar frameworks do not allow it.
- **Review privacy policies before adopting a new tool.** Specifically check data retention, training use, and how to delete your data.
- **When in doubt, ask.** Contact AXICOM before adopting a new AI tool or before uploading anything sensitive.

Approved AI Tools

- **Microsoft Copilot (M365):** approved for general business use within your tenant. Data is protected under Microsoft's commercial data-protection terms. Copilot Chat is included for free; Microsoft 365 Copilot requires additional licensing.
- **Other AI tools:** review with AXICOM before use, especially for any task involving client, financial, or regulated information.

Questions or Need Help?

AXICOM is here to help your team adopt AI safely. If you are unsure whether a tool or use case is appropriate, please reach out before uploading anything.