QUICK REFERENCE

AI Acceptable-Use Quick Reference

What every employee needs to know before typing anything into ChatGPT, Copilot, or Gemini.

The Four Golden Rules

Rule 1 — Never put confidential information into AI

Customer lists, credit card numbers, Social Security numbers, medical records, employee personal information, or confidential client data should never be pasted into ChatGPT, Copilot, Gemini, or any other AI tool. Once data goes in, you have lost control of it.

Rule 2 — Always review AI output before using it

AI hallucinates. It makes up facts, regulations, and citations that sound confident but do not exist. Verify anything legal, financial, medical, or compliance-related against a trusted source before acting on it.

Rule 3 — Anonymize before analyzing

If you need AI help on customer data, strip it first. Replace names, addresses, phone numbers, and emails with "Customer A", "Customer B", and so on. The AI still gets the pattern; the people stay private.

Rule 4 — AI assists, humans decide

Never let AI make final decisions on hiring, firing, credit, or anything else with real consequences for a real person. Use it to brainstorm questions or summarize inputs — then decide yourself.

Safe Uses vs. Risky Uses

- ✓ **Safe:** Drafting marketing copy, blog posts, social media
- ✓ **Safe:** Summarizing long non-sensitive documents
- ✓ **Safe:** Brainstorming ideas, outlines, or campaign concepts
- ✓ **Safe:** Translating text that contains no personal data
- ✓ **Safe:** Drafting code (with a human code review before production)
- ✗ **Risky:** Processing credit card numbers, SSNs, or bank details
- ✗ **Risky:** Uploading medical records or health information
- ✗ **Risky:** Making hiring, firing, or credit decisions from AI output
- ✗ **Risky:** Pasting client-confidential information into public AI tools
- ✗ **Risky:** Claiming AI-generated content is entirely human-written

Before Approving a New AI Tool, Ask:

- ✓ Where does my data go — stays on device, or sent to company servers?
- ✓ Is my data used to train the AI, or is it fenced off from training?
- ✓ How long is data kept, and can I delete it on demand?
- ✓ Can employees of the AI company see my data?
- ✓ What country are the servers in, and what privacy laws apply?

Simple AI Policy Template

Approved tools: [list the ones your company has vetted — e.g., Microsoft Copilot, ChatGPT Team, Google Workspace AI]

Rules for every employee:

- Never input customer or employee personal information
- Never input financial account details of any kind
- Always review AI output before using it externally
- If you want to use a new AI tool, ask [designated person] first
- When in doubt, treat AI like a paid contractor you do not fully trust

Violations: Honest first-time mistakes are teaching moments. Repeat or intentional violations trigger formal discipline.

Red Flag Behaviors to Watch For

Employees using unauthorized AI tools. Someone presenting AI-generated content as their own. AI being used for sensitive decisions without human review. Customer information being pasted into public tools. Employees bypassing security controls to reach AI services.