

Using AI at work

Our AI use policy on one page: what to do, what never goes in, and what to check before anything leaves the team.

OUR APPROVED TOOLS

YOUR CHECKER

QUESTIONS AND SLIPS

NEVER PUT THESE INTO AN AI TOOL

- **Never put personal data into an AI tool:** names with contact details, ID numbers, health or HR records **[and customer records]**.
- **Never put passwords and security details into an AI tool:** passwords, access codes, keys, anything that lets someone in.
- **[Never put any item our policy adds into an AI tool: copy it here in the same words.]**
- **[Our one exception, if the policy keeps it: a tool the register approves for that kind of information. Never passwords.]**
- **Never put client confidential material into an AI tool:** anything a client shared in confidence, or that a contract covers.
- **Never put unreleased financials into an AI tool:** results, forecasts, budgets, prices and deals not yet public.

DO

- **Use the approved tools,** signed in with your work account.
- **Brief it.** Say the goal, what done looks like, and what it must not touch.
- **Give it the source.** Paste in the real text, as long as it isn't on the never list. With the real text in front of it, the likely answer is usually the true one. Usually, not always: still check.
- **Ask it where.** Have it quote the line or link the page, so you can check it.
- **Say when AI did a large part of a piece of work.**

DON'T

- **Don't use a personal or free account** for work.
- **Don't connect a tool** to email, files or calendars without approval.
- **Don't let an AI agent send, pay or delete** without asking you first. That is set in the tool. New agent tasks start at Read or Draft.
- **Don't record or transcribe a meeting with AI** without telling everyone first.
- **Don't let AI decide about a person.** A person decides, and can explain it.

CHECK

- **Read all of it,** not just the start.
- **Check every fact, figure, name, quote and link** outside the chat. Quotes and links can be invented too.
- **Don't ask it "are you sure?"** That isn't checking. Check outside the chat.
- **Make sure nothing from the never list** slipped in.
- **Would you put your name to it?** If not, it doesn't leave the team.

WHY WE CHECK

An AI tool writes a likely answer, and likely isn't the same as true.

OUTSIDE TEXT

Words planted in a web page, an email or a document can get treated as an instruction. It's called prompt injection.

NOT SURE?

Leave it out, or ask first. Slipped up? Tell your contact above the same day.