

What Never Goes into an AI Tool

For everyone at [Organization Name] who uses AI for work. Questions? Ask [IT contact name, email or channel].

Before you start

- **Check with your IT team.** Ask what [Organization Name] allows before you put anything from work into an AI tool.
- **Use an approved tool.** Only the tools listed at [Approved AI Tools List URL or location].
- **Sign in with your work account.** It keeps your chats inside the agreement [Organization Name] signed. A personal account sits outside it.
- **Connected apps.** An email or file connection IT approved can read the names and addresses in what it opens. Everything else on this page still applies.
- **No approved account yet?** Practice with made-up text, or on paper, until IT gives you one.

Never put this into an AI tool

- **Customer or personal details.** No names, email addresses, phone numbers, home addresses or account numbers, for customers or colleagues.
- **Regulated records.** Health, financial, HR and legal records stay in their own systems, unless IT has told you in writing that this tool may see them.
- **Passwords, keys and access codes.** No credentials of any kind, and nothing that grants access to a system.
- **Anything under an NDA or not yet public.** Unreleased plans, contracts, pricing and source code need clearance first.
- **Anything our policy prohibits.** If the AI use policy keeps it out, it stays out.

Do this instead

- **Swap real details for placeholders.** Write "Customer A", "[client name]", "\$X". Put the real details back yourself.
- **Describe the situation.** An AI tool needs the shape of the problem, not the file it arrived in.
- **Trim a file first.** Remove identifying columns and pages, or use a short extract.

Check the answer before you use it

- **Read it as if a colleague had drafted it.** AI tools state wrong things with complete confidence. The check is yours.
- **Say where AI helped.** Follow [Organization Name]'s rule on disclosing AI assistance.

When you are not sure

- **Ask before you paste or upload, not after.** A question to IT takes a minute.
- **When in doubt, leave it out.** If you would not email it to someone outside [Organization Name], keep it out of the chat.
- **If something went in by mistake,** stop and report it to [IT incident email]. Reporting in good faith is always the right call.