doingit.today

Checklist · 4 min read

What never to paste into AI

A one-page checklist for work and home. What's fine to type into an AI tool, what should never go in, and how to make something safe before you paste it.

The one-line rule

If you wouldn't put it on a postcard, or email it to someone outside your organisation, don't paste it into an AI tool until you've checked the rules.

Why be careful? When you use an AI chat tool, what you type is sent to the company that runs it. Depending on the tool and its settings, your chats may be stored, seen by staff checking for misuse, or used to improve future versions. Paid work versions usually have stronger promises, which is why many employers approve one tool and ban the rest.

THIS IS A GUIDE, NOT LEGAL ADVICE

Your employer's policy and your contracts come first. If they say something different from this page, follow them.

Never paste these

- ✗ **Passwords, PINs and security answers.** No AI tool needs them. Ever.
- ✗ **Bank, card and payment details.** Yours or anyone else's.
- ✗ **Government ID numbers.** National Insurance, passport, driving licence, tax references.
- ✗ **Other people's personal details** unless your organisation has approved the tool for that: names with addresses, phone numbers, dates of birth, health, pay or performance.
- ✗ **Health records and anything about a patient or client's care.**
- ✗ **Details about children or pupils** that could identify them.
- ✗ **Client or customer information you hold in confidence**, including anything under a non-disclosure agreement.
- ✗ **Company secrets:** unannounced plans, prices not yet public, source code, contracts, figures before they're published.

- ✗ **Legal matters in progress:** disputes, complaints, disciplinary cases.

Usually fine

- ✓ General questions and explanations: "How does a balance sheet work?"
- ✓ Your own writing that isn't confidential: a draft blog post, a talk, a cover letter
- ✓ Public information: text from a public website, a published report
- ✓ Made-up or anonymised examples (see the next section)
- ✓ Your own ideas, plans and to-do lists, with other people's details left out

Make it safe first: five swaps

Often you can get the same help without the private parts. Before you paste, swap them out.

INSTEAD OF	TYPE
A real name	"Customer A", "my manager", "a supplier"
A company name	"a mid-sized retailer", "Client X"
Exact figures	Round numbers or "about 20% up"
A whole document	Only the paragraph you need help with
A real case	"A customer in this situation: …" with the details changed

PROMPT 1

Ask for a template, not an answer about real people

You need help with a sensitive email or document.

Write a template for **[the kind of message, e.g. a letter telling a customer their complaint was not upheld]**. Use placeholders in square brackets for every name, date, amount and specific detail. Keep the tone **[calm and respectful]**.

Tip: Fill in the real names and details yourself afterwards, outside the AI tool.

PROMPT 2

Get it to help you strip the details out

You have notes you'd like summarised, and they mention real people.

> I want to anonymise text before sharing it. Here is a made-up example: **[paste a harmless example]** . Show me which parts would identify a person or organisation, and rewrite it with neutral labels such as "Person A" and "Company X".

Tip: Do the swap yourself first for anything truly sensitive. This prompt is for getting the method right on a harmless example.

Five questions to ask at work

1. **Which AI tools are we allowed to use?** Many organisations approve one and block the others.
2. **What can go into it?** Ask for the short version: public only, internal, or confidential too.
3. **Is our version set so that chats aren't used for training?** Work plans often are. Personal free accounts often aren't by default.
4. **Do I need to say when I've used AI?** Some clients, schools and regulators expect you to.
5. **Who do I tell if I paste something I shouldn't have?** Tell them quickly. It's much easier to sort out early.

If you've already pasted something

1. Don't panic. One slip is common, and most can be tidied up.
2. Delete the chat. Look in the tool's settings for a way to delete your history as well.
3. If it was a password, change it now. If it was a card number, call your bank.
4. If it was work or client information, tell your manager or data protection lead today.

Want your whole team on the same page?

doingit.today maps how your team works, then teaches everyone the AI steps in the tools you're allowed to use. Start with one job of your own.

Free to start. No tech background needed.

Start free at doingit.today

Read more from the people who set the rules

- The UK's National Cyber Security Centre on ChatGPT and large language models: what's the risk?
- Your AI tool's own privacy page and data controls, in its settings.

Free to share and print, with this line kept on. AI tools make mistakes, so check anything that matters before you use it. doingit.today is run by DoingIt Limited, registered in England and Wales, company number 17108880. The tool names belong to their owners.