

# What not to paste into an AI tool

AI Tools Field Guide Not affiliated with OpenAI, Google, xAI or Anthropic; your organization's rules come first.

**Public tools take public material. A work account may take more, within its rules. Secrets and other people's data go in neither.**



## Three tiers, three rules

- **Public tools.** The free or personal ChatGPT, Gemini, Grok or Claude take public material only. Never put personal data, internal details, or anything not shareable into a public tool.
- **A work or enterprise account.** Your organization's approved tier can take more, within its own rules and data-use agreement.
- **Never, anywhere.** Secrets, credentials, and other people's private information stay out of any AI tool.



## Why a work account is different

- **Contracted and logged.** An enterprise agreement sets retention and training terms that differ from the free consumer app.
- **Not used for training.** Under most business terms, your organization's data is not used to train the model, unlike the free tier by default.
- **Not private either.** Chats can be visible to administrators and logs. Treat a work-account chat like a work email.



## Before you upload

- 1 **Name the data.** Public, internal, personal, or secret? A file often mixes them.
- 2 **Take the sensitive columns out.** Bios for an awards package are fine; a roster with personal identifiers is not.
- 3 **Apply the share-drive test.** If the file would be a problem on your shared drive, it is a problem here too. Sensitive material goes only into an approved account, within your organization's guidance.
- 4 **If something slipped:** tell your IT or data-security lead. They decide next steps.

### TAKE AWAY

**Public tools take public material. A work account may take more, within its rules. Secrets and other people's data never. When in doubt, ask before you upload.**

An independent site to help people learn what generative AI is and how to use AI tools well. It is not official guidance from any organization. Platform, vendor, and policy facts change quickly, so follow your own organization's rules and verify anything you rely on. Use at your own risk.