

PRINTABLE GUIDE

Use an AI privacy checklist

AI services have different privacy policies, storage choices and connected tools. 'Safe to use' depends on the task and what you share. This checklist keeps an ordinary drafting or explanation exercise useful without giving it unnecessary personal information.

Phone or computer | 2 min read | 5 steps

Before you start

- ☐ Use the genuine service and read its current privacy information.
- ☐ Choose a small task such as rewriting a non-private paragraph.

1. Leave secrets out

Do not enter passwords, login codes, full payment-card details or recovery keys. Replace identifying details with labels such as 'customer' or 'my town' when the exact information is unnecessary.

- ☐ Done this step

2. Check files before uploading

Look for personal details, confidential work information and other people's data. Use a cleaned copy or short invented example if it serves the same purpose. Follow your employer's data rules.

- ☐ Done this step

3. Read the service's data choices

Find its privacy and account settings. Check how content is stored, shared or used and what deletion options mean. Do not assume the settings of one provider apply to another.

- ☐ Done this step

4. Review tool permissions

Only connect accounts needed for the task. Read access requests carefully. If an assistant can act in another service, make clear which actions need your review before they happen.

☐ Done this step

5. Inspect the result before using it

Check factual claims and remove unintended personal details. Review drafts before sending them. For high-stakes decisions, use suitable authoritative guidance rather than relying on a chatbot alone.

☐ Done this step

Try it for yourself

Rewrite a private example using fictional names before asking AI for help.

☐ I tried the task.

My notes

Does deleting a chat guarantee every copy disappears immediately?

Do not assume so. Storage, retention and deletion rules depend on the provider and service. Read the current policy before sharing sensitive material.

Official help and the online guide

NCSC advice on sensitive AI prompts -

<https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk>

Official OpenAI documentation: permissions - <https://learn.chatgpt.com/docs/permissions>

Read online: <https://plaintech-guides.pages.dev/guides/use-an-ai-privacy-checklist/>