

PRINTABLE GUIDE

Check a prompt before sharing it with AI

Remove private details before using AI. Privacy terms vary; check prompts and attachments, including information about other people.

Any AI chat or writing tool | 2 min read | 5 steps

Before you start

- ☐ The prompt or attachment you intend to submit
- ☐ A task that can use fictional or anonymised details

1. State the task without secrets

Write the practical job, such as drafting a polite reply or explaining a term. Leave out passwords, PINs, security codes, recovery codes and full payment-card details. A useful example rarely needs a real account secret.

- ☐ Done this step

2. Replace identifying details

Use invented names and example addresses instead of real contact details, identification numbers or account references. Removing a name alone may not anonymise a story if dates, locations and other details still identify someone.

- ☐ Done this step

3. Inspect attached material

Read pasted text and look through each page or image. Check document headers, background details, messages and signatures. Do not upload private workplace, client or family material without the right authority and an appropriate service.

- ☐ Done this step

4. Check the service's controls

Read the tool's current privacy and data-handling information. Retention, training and sharing settings differ by account and service. A familiar brand or private-looking chat does not establish how submitted data is handled.

☐ Done this step

5. Submit only what is necessary

Give the smallest amount of information that lets the tool perform the task. Review its response before using it. If you accidentally disclosed a secret, use that account's genuine security process to replace or revoke it; deleting a chat is not a substitute.

☐ Done this step

Try it for yourself

Rewrite a practice prompt using fictional names and no account or payment details.

☐ I tried the task.

My notes

Can I paste a bank or medical letter for a summary?

Use an example or remove identifying and sensitive details first. For sensitive documents, choose an authorised service with data handling suitable for that task.

Official help and the online guide

NCSC: sensitive information in AI prompts -

<https://www.ncsc.gov.uk/sites/default/files/pdfs/blog/chatgpt-and-large-language-models-whats-the-risk.pdf>

Read online: <https://plaintechguides.com/guides/ai-private-information-checklist/>