

AI PRIVACY CHECKLIST

Before you paste, upload or connect anything to an AI assistant

NEVER SEND

- Passwords, API or encryption keys, and recovery codes
- Government IDs; card or bank account numbers
- Medical, genetic or biometric data
- Third-party or client data without permission or a legal basis
- NDA material, internal code or unreleased results
- Intimate information or precise location data

CLEAN FIRST

- Reduce the input to the minimum fragment the task needs
- Replace names and identifiers with clear placeholders
- Prefer synthetic examples over real records
- Remove visible data and hidden metadata, comments and history
- Reopen the cleaned file and verify every page or sheet

ACCOUNT CHECK

- Is this a consumer account or an approved work account?
- Check training, chat history and retention controls
- Know what Temporary or Incognito modes do - and do not do
- Review connected apps, files, drives and permissions

IF YOU ALREADY SENT IT

- Delete the chat, shared link and uploaded file where possible
- Revoke connector or app access
- Rotate exposed secrets and end active sessions
- Contact your bank or card issuer if financial data was exposed
- Notify security, privacy or DPO contacts at work
- Assess breach notification and other legal duties

30-SECOND YES / NO CHECK

● Does the AI need this exact detail?

● Is it mine to share?

ALL YES → Share the minimum, cautiously.

● Is this account approved for it?

● Did I clean and reopen the file?

ANY NO OR UNSURE → Stop and use a safer route.

Settings reduce risk; they do not make sensitive uploads automatically safe.

If the AI does not need a detail, do not send it.