

Set up ChatGPT with privacy in mind

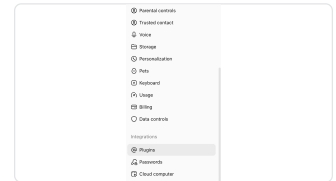
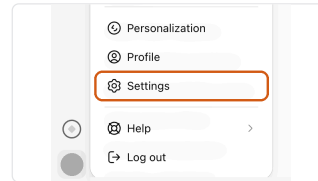
Four checks, about ten minutes. This is for your own ChatGPT account. These settings reduce risk.

They do not make a personal account an approved place for confidential board or company information.

Start here: find your settings

Click your initials at the bottom left, then Settings.

Connected apps live under Settings, then Plugins.

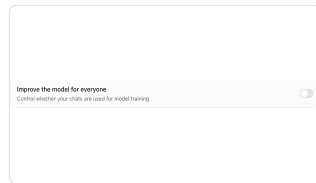
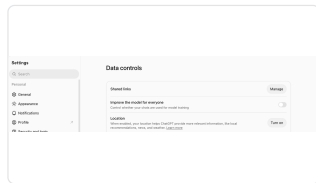


1 Stop your chats being used to improve the AI

Do this:

- Go to Settings, then Data controls.
- Switch off "Improve the model for everyone".

Why: OpenAI can use your chats to improve its AI. Switching this off stops that for new chats. Avoid rating a reply with thumbs up or down: it can still share that chat, even with this switch off.

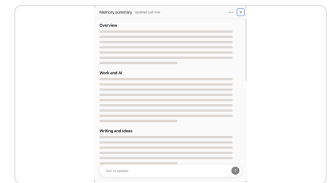
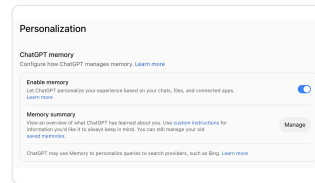


2 Decide what ChatGPT remembers

Do this:

- Go to Settings, then Personalization.
- Check the "Enable memory" switch is how you want it.
- Choose "Manage" under Memory summary to read what it holds. To remove something, tell the chat box what to forget. To remove all, use the three dots and "Delete and turn off memory".

Why: memory learns from your chats, files and connected apps. That makes ChatGPT more useful and means it holds more about you. To remove something fully, you may also need to delete its source chats or files.

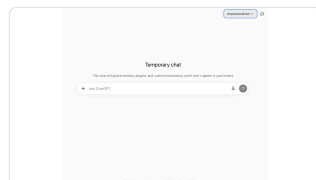
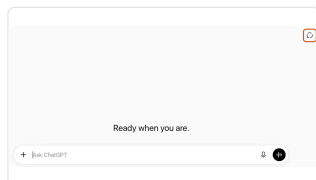


3 Use a Temporary Chat for private questions

Do this:

- In a new chat, press the chat icon with a dotted outline at the top right.
- Choose "Unpersonalized" before your first message. The default, Personalized, still uses your memory.

Why: an Unpersonalized Temporary Chat stays out of your history and ignores your memory, plugins and custom instructions. It is not used to improve the AI. The company may keep a copy for up to 30 days for safety. Use it when you'd rather ChatGPT didn't remember a question, such as a health query or how to handle a difficult conversation. Keep board and company material out of it, even here.

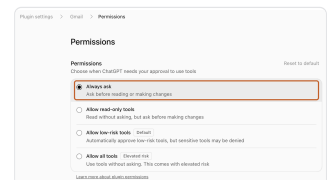
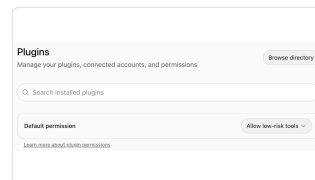


4 Connect with care, and keep control

Do this:

- Keep board or company emails in a separate account it can't reach.
- Connect one at a time, and only if it saves real time.
- Go to Settings, then Plugins. Open each plugin, such as Gmail, and set its permission to "Always ask". Avoid "Allow all tools": it uses tools without asking.
- To stop a plugin's access, open it and press "Uninstall". For one account, use the three dots next to it and choose "Disconnect". Neither erases what is already in your chats.

Why: once you connect your email or diary, ChatGPT may be able to reach sensitive information in that account, board papers included, depending on the permissions you give.



Check again once a month

Put a reminder in your diary for the first Monday of each month. Check the privacy setting is still off, review what is connected and read what ChatGPT remembers. This prompt helps with the last one:

What do you remember about me? List it all, grouped by topic, and flag anything that looks sensitive.

Also: protect your login. Under Settings, then Security and login, add a passkey, switch on multi-factor authentication and log out of any devices you don't recognise. **Using a company account?** Your workspace administrator controls many of these settings, so ask them how yours is set up.