AI Privacy Settings Guide

A practical starting point for insurance broker teams using personal ChatGPT or Claude accounts.

The most important point

Turning off model-training controls is useful, but it does not make it appropriate to paste unrestricted client information into a public AI service. Settings can change how content is used; they do not remove the need for an approved business procedure, data minimisation and human review.

Before changing settings

Confirm which AI products and account types staff are using. A personal paid subscription is not the same as a centrally managed business workspace. Decide which tools are approved for work, who owns the account and what categories of information staff must never enter.

ChatGPT: personal Free or Plus account

1. Open your profile menu and choose **Settings**.
2. Open **Data Controls**.
3. Turn off **Improve the model for everyone** if the business does not want new conversations used to improve models.
4. For a conversation that should not remain in history or create memories, start a **Temporary Chat** before entering any content.

Temporary Chat is not a permission to enter client data. OpenAI states that Temporary Chats are not used to train models and are deleted from its systems after a limited period, but copies may be retained for safety purposes during that period. Check the current product notice before relying on it.

Claude: personal Pro account

1. Open your profile and choose **Settings**.
2. Open the privacy or data controls available for the account.
3. Turn off the option that permits chats to be used to improve Claude where that control is available.
4. Use an **Incognito chat** where appropriate, while continuing to follow the business rule on client information.

Names and locations of controls can change. If the menu shown in this guide is different, stop and check the provider's current privacy documentation rather than assuming the old setting still applies.

Settings are only one part of safe use

A five-point check for broker teams

Question	Minimum practical control
Which tools are approved?	A named list of approved products and account types.
What must not be entered?	A plain-English rule covering client-identifying, financial, claims and health information.
Who checks the output?	A staff member remains responsible for verifying facts, figures, coverage wording and correspondence.
Who checks settings?	A named person reviews account controls and provider changes regularly.
What happens when staff are unsure?	They stop, remove the client information and ask the responsible person.

A rule staff can remember

Do not enter client-identifying information into an AI tool unless the business has expressly approved that tool, account and use. Remove names and unnecessary detail. Treat health, claims and financial information with particular care.

Use AI as an assistant, not the decision-maker

AI can help organise ideas, improve general wording and explain unfamiliar concepts. It can also invent facts or produce confident but incorrect answers. Staff should verify every material statement and must not rely on AI to make an insurance, compliance, legal or customer decision.

Check current guidance

Product controls and retention practices change. Review the provider documentation whenever an account plan changes and at regular intervals.

OpenAI: help.openai.com - Data Controls FAQ and Temporary Chat FAQ
Anthropic: privacy.claude.com and support.claude.com - privacy controls and Incognito chats

Important: This is practical training guidance, not legal, regulatory, data-protection or cybersecurity advice. Each firm must assess its own systems, contracts, processing activities and obligations.