AI Privacy and Security CHEAT SHEET

Plex Consulting

Personal Use: Stay Private and Safe

- **Use trusted, reputable AI tools** — stick to well-known platforms (ChatGPT, Claude, Gemini) with published privacy policies.
- **Upgrade to Pro or paid versions** — paid tiers typically disable training on your data and offer stronger privacy controls.
- **Never paste confidential data into free tools** — free AI services may use your inputs for model training. Assume anything you type is retained.
- **Turn off chat history and training** — most platforms let you opt out of data retention in settings. Do this immediately.
- **Regularly export and delete your data** — periodically download your AI conversation history and then delete it from the platform.
- **Start with safe, low-risk tasks** — use AI for general research, writing improvement, and brainstorming before handling anything sensitive.

Questions to Ask Your IT Team

- **Who has access to AI tools?** — understand which roles are approved and whether access is centrally managed.
- **Free vs enterprise: what is sanctioned?** — clarify which tools are approved for corporate use vs personal experimentation.
- **Where does our data go?** — ask whether AI vendors store, process, or train on your organisational data.
- **Do we have an AI acceptable use policy?** — if not, advocate for one covering data classification, approved tools, and prohibited uses.
- **Is AI usage being tracked?** — enterprise tools should provide audit logs, usage dashboards, and cost tracking.
- **Are audit trails and MFA in place?** — AI platforms should integrate with SSO, enforce MFA, and log all interactions.

Good to Know

- **Generative AI predicts the next word** — it does not "understand" things. It generates statistically likely continuations of your prompt. This is why it can hallucinate confidently.
- **Pro and paid tiers disable training** — ChatGPT Plus, Claude Pro, and Gemini Advanced all commit to not training on your data. Free tiers typically do not.
- **Paid plans include admin controls** — enterprise and team plans provide user management, SSO, data residency options, and usage analytics that free plans lack.
- **RAG keeps your data internal** — Retrieval-Augmented Generation lets AI search your own documents without sending them to external servers. The safest way to use AI with proprietary data.
- **The right question matters more than the tool** — asking "should we put this data in AI?" is more important than which AI you choose.