Is This AI Tool Safe? A Quick Checklist

Before you install an AI app or browser extension, click 'connect my account,' or let a vendor's AI touch your data, run through this.

FIRST, KNOW WHAT KIND OF AI YOU'RE LOOKING AT

The big chat apps	The developer / API side	AI baked into a product you already use
(ChatGPT, Claude, Gemini). This checklist is mainly for these. Most of your day-to-day AI use lives here.	Same companies, but a more technical, more configurable path. Different data handling. If someone on your team is building with this, it needs its own review.	Your CRM, scheduler, email tool, or other vendor may have added AI. It might run on one of the big three, or something else entirely. You usually can't tell from the outside - you have to ask. See the vendor section below.

The 5-point check (any new AI tool)

1. **Who makes it?** Is there a real, identifiable company behind it, with a findable website and contact (not just an anonymous app)?
2. **What permissions is it asking for?** Do they match what the tool actually does? A note-taker does not need your full inbox and calendar.
3. **What does its privacy policy say about your data?** Look for whether your data is stored, sold, or used to train AI, and whether you can opt out.
4. **Is it free?** If yes, ask what they get in return. Often the answer is your data. 'Free' is not automatically bad, but it is a reason to look closer.
5. **Does someone reputable stand behind it?** An established name, real reviews, or a recommendation from someone you actually trust.

Red flags (stop and ask first)

- Asks for your password to another service, instead of an official 'Sign in with Google/Microsoft' button.
- Wants broad access ('read and change everything') for a small, simple task.
- No company name, no privacy policy, or a site full of typos and urgency.
- A browser extension that wants to 'read and change all your data on all websites.'

Before you click 'connect'

Connecting an AI tool to your Gmail, Drive, or other account usually grants ongoing access until you revoke it (not a one-time peek). Treat it like handing over a key to the building, not a glance through the window. Only connect tools you would trust with that key.

If a vendor's product has AI built in, ask them

You often can't tell what is running under the hood, so ask the vendor directly. Good vendors will have ready answers.

- **Whose AI is it?** One of the big providers, or something else? Is any of our data sent to that AI provider?
- **Where does our data go, and is it stored?** Does it stay within your system, or get sent out for processing?
- **Is our data used to train any AI model?** Can we turn that off?
- **Can we turn the AI feature off entirely** if we decide we don't want it?
- **If we handle sensitive information,** do you offer the agreements and settings needed for that? (Then take their answer to your own leadership and advisors.)

Our team rule

New AI tools (and new AI features in existing products) get approved by one named person before anyone installs, connects, or turns them on.

Owner: _____

For general staff guidance only. Not legal advice. Anything involving real client or medical information is a conversation for your leadership and advisors. When in doubt, don't connect the tool - ask first.