

AI Tools Field Guide Not affiliated with OpenAI, Google, xAI or Anthropic; your organization's rules come first.

Most failures are a missing source or an unchecked claim.



! It does not know

- **Your command.** Confident answers about your instruction or roster when nothing was attached. Attach the source.
- **This year.** Its knowledge has a cut-off, and web search is a periodic index. Attach the current version, or keep it in a project so every chat has it.
- **Arithmetic.** Watchbill counts and per-diem that look right and were never computed. Make it write the formula, or use a tool that computes: Grok's skills, Excel, PowerShell.
- **Page 60 of 100.** Long files are read unevenly. Attach the section, or ask about it by name.

🗨️ It invents

- **References** in the right format that do not exist or do not say that. Make it quote the sentence; a second chat checks each one against the file.
- **A complete-looking answer** with the gaps filled in fluently. Ask "what is missing from the source?"
- **A version you rejected,** returned to in a long chat. Start fresh with only the source and the request.
- **Instructions hidden in a document** it read as if you had typed them. Treat outside files as untrusted; a person reviews before anything acts.

📋 Habits that prevent most of it

- 1 **Give the source** and say that "not in the source" is an acceptable answer.
- 2 **Ask for references beside each claim** and check the ones you will act on.
- 3 **Pick the careful model** for anything you will brief or sign.
- 4 **Keep to the data rules:** public tools take public material, a work account may take more within its rules, secrets and other people's data never.

TAKE AWAY

It is a language processor, not a knowledge store. Source in, references out, your eyes on what matters, and most of this list never bites.

An independent site to help people learn what generative AI is and how to use AI tools well. It is not official guidance from any organization. Platform, vendor, and policy facts change quickly, so follow your own organization's rules and verify anything you rely on. Use at your own risk.