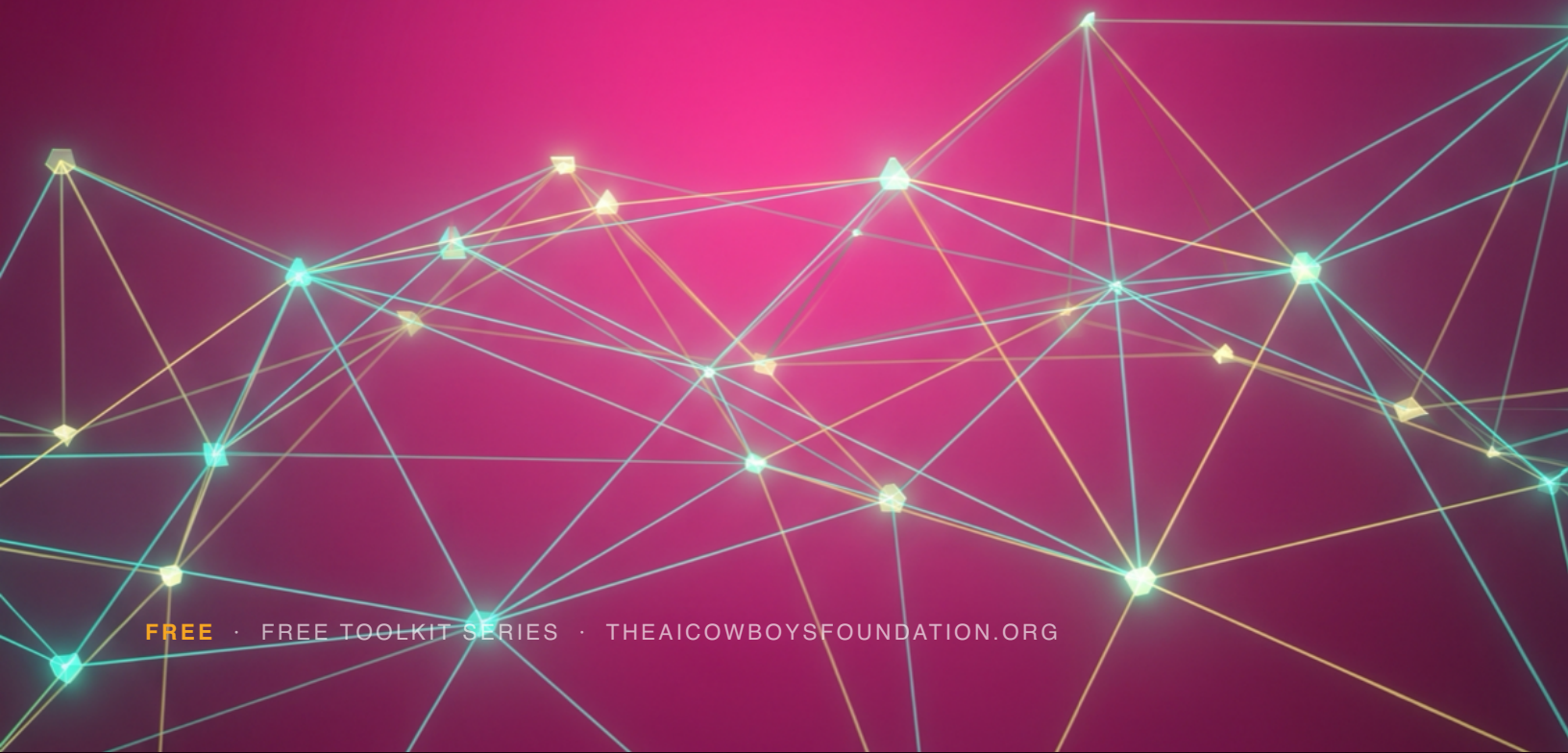
THE AI COWBOYS FOUNDATION

TOOLKIT 06 · PRIVACY

Data Privacy Quick Reference

Keep sensitive information out of the wrong place. One page, three questions, zero leaks.



Data Privacy Quick Reference

The most common AI leak is not a hack. It is a helpful paste into the wrong tool.

A one page guide to keeping sensitive information out of the wrong place. Print it, pin it near your desk, and check it before you paste anything into an AI tool.

The most common AI privacy failure

The most common way sensitive information leaks through AI is not a hack. It is a helpful employee pasting a real document into a free consumer tool to save time. The tool may store what was typed, learn from it, or surface it in ways nobody can undo. One minute of caution prevents almost all of it.

3

questions to ask before you paste anything

0

personal or confidential details belong in a consumer tool

24 hr

is a good window to report any suspected exposure

WORKED EXAMPLE: FIX A RISKY PASTE IN TEN SECONDS

Risky: `Summarize this complaint from Maria Gomez, account 4471, about a billing error on her March invoice of $842.`

Safe: `Summarize this customer complaint about a billing error on a recent invoice.` Then add the specifics yourself, or use an approved tool with a signed data agreement.

Same help, no exposure. You removed the name, the account number, and the dollar figure, and the summary is just as useful.

REAL WORLD: TEXAS REQUIRES THE NOTICE

Privacy expectations around AI are becoming law. In Texas, Government Code 2054.711 requires state agencies and local governments to display a standardized public notice whenever an AI system is public facing or is a controlling factor in a consequential decision. The Texas Department of Information Resources also publishes a statewide AI acceptable use policy that pairs data rules with every approved use.

The lesson: transparency about AI and discipline about data now travel together. The habits on this page are the personal version of what the largest employers in Texas are required to do.

Never paste these into a consumer AI tool

- Names, addresses, or contact details of real people
- Health, financial, legal, or benefits records
- Government identifiers or case numbers
- Passwords, keys, or security details
- Anything a client or partner shared in confidence
- Anything marked internal, sensitive, or confidential

Safer by default

- Use an approved tool with a signed data agreement for anything work related.
- Use your organization account, not your personal one.

- Turn off chat history or model training on your data where the tool allows it.
- Remove names and details before you ask for help with a real document.
- Ask for general guidance, then apply it to the specifics yourself.

Three questions before you paste

1. Would I be comfortable if this text appeared in public?
2. Does this include information about a real, identifiable person?
3. Is this tool approved for this kind of information?

If the answer to question 1 is no, or question 2 is yes, or question 3 is no, stop and ask your AI lead.

If something is exposed

- Stop using the tool for that data right away.
- Tell your AI lead or security contact promptly, within [time, for example 24 hours].
- Write down what was shared and when, so it can be reviewed.

Why this matters

AI tools can store what you type, learn from it, or expose it in ways that are hard to undo. A minute of caution protects the people who trust you with their information, and it protects your organization's name.

Sources and further reading

- Texas DIR AI templates and resources, Texas Department of Information Resources
- NIST AI Risk Management Framework, National Institute of Standards and Technology
- NIST AI Resource Center, National Institute of Standards and Technology

PUT THIS TO WORK

Want help applying this in your organization?

The AI Cowboys Foundation delivers free briefings, workshops, and readiness assessments for business, government, classrooms, and veteran programs. Tell us what you are working on and we will point you to the right next step.

Contact us

roger@theaicowboys.com · theaicowboysfoundation.org/contact