A LONG, HONEST LETTER

Your AI, on *your* terms

Keeping your work yours — what's actually safe, and the strange new world of open-source AI.

You can use the AI tools you already love *and* keep your work yours. Both things can be true.

IF THIS SOUNDS FAMILIAR

If you've started using AI in your work, you've probably felt it — the small worry underneath the convenience. You paste in a client email to get help with a reply, and a quiet voice in the back of your mind asks: *where does this actually go?*

So you go looking for a straight answer. And you can't find one. One article says stop worrying, the big companies have your back. The next says it's hopeless, they're already trained on everything you've ever typed. The settings pages are a maze. The terms of service are forty pages of fog.

So you do the reasonable thing — you half-use it. You keep the real work out of it, you don't dig in, and you never quite get the payoff everyone keeps promising. The not-knowing is the thing holding you back.

What I want to give you here is the straight answer. The conversation has been split into two unhelpful extremes: *"use everything"* and *"trust nothing."* The honest version lives in the middle — and it's genuinely doable.

> *Two things can be true. AI can be powerful AND yours.*

That's the whole letter. The fix is fast — most of it takes about ten minutes. The habits that keep your business yours come after, and they're doable too.

START WITH THE MAP

Almost every decision lives in *one of three tiers.*

Knowing which tier you're operating in matters more than any single setting. Here's the picture the way I'd draw it on a napkin.

TIER	WHAT IT IS	RIGHT FOR
1 · Cloud Default	Use the tools as-is, settings untouched. **Lowest privacy.**	Casual queries, public content
2 · Cloud Locked Down	Same tools, training off, Projects on, "never paste" discipline. **High privacy, 10–15 min.**	Daily small-business work
3 · Truly Local	AI running entirely on your laptop, no cloud. **Highest privacy.**	Regulated data, deep needs

> *Tier 2 is where almost every woman business owner should live.*

You get the power of the big cloud models — the polish, the speed — and your business stays inside a container that doesn't feed somebody else's product.

THE TEN-MINUTE LOCKDOWN

Flip these once. Your work stops becoming *training data.*

Open each tool in another tab and walk through as we go. This is the most useful ten minutes in this letter.

ChatGPT	Settings → *Data Controls* → "Improve the model for everyone" → **OFF.** Turn on Temporary chats for anything sensitive.
Claude Anthropic	Settings → *Privacy* → "Help improve Claude" → **OFF.** Worth re-checking every few months.
Gemini Google	Settings → *Activity* → "Gemini Apps Activity" → **OFF,** or auto-delete every 3 months.
Copilot Microsoft	Settings → *Privacy* → "Model improvement" → **OFF.** Check which account is signed in.
Apple Intelligence	Most work happens on-device; some routes to *Private Cloud Compute* — one of the better designs out there. Worth knowing it exists.

→ The *"never paste"* list

Even with every toggle flipped, some things just don't belong in cloud tools. Ever. This matters more than any single setting.

- Real names of family members – *I use "my son," "my friend"*
- Specific medication doses; address, phone, SSN, DOB, bank numbers
- Actual dollar amounts – *I use ranges, like "low five figures"*
- Client names – *"Client A," "Client B"* · anything under NDA or HIPAA
- Login credentials of any kind, ever

→ Keep your work *contained*

The bigger move is structural – keep your business inside a private workspace, not scattered across forty random chats.

- **Claude Projects.** A private workspace with its own knowledge base. Upload your brand voice, SOPs, past emails – every chat starts knowing your business, and nothing leaks into training.
- **ChatGPT Custom GPTs.** Same principle. A saved configuration for a specific job, with private knowledge files and a system prompt that knows who you are.
- **The Claude desktop app.** Reads files off your hard drive with your permission. For confidential client work, the file never has to leave your machine.

RUNNING AI ON YOUR OWN LAPTOP

The option exists. Most people *don't need it.*

When you run AI locally, the model lives on your computer. Your question never leaves your machine. No cloud server, no company logging anything.

- **LM Studio.** A visual app, no terminal. Download a model from inside it and chat like ChatGPT. The easiest entry point.
- **Ollama.** One command, one model running — for anyone comfortable in the terminal. Free, open source.
- **Open WebUI.** A polished ChatGPT-like interface for your local models. More setup, much nicer.

YOUR COMPUTER	WHAT IT CAN COMFORTABLY RUN
Apple Silicon (M1–M4), 16GB+	Small-to-medium models, comfortably
Recent Windows GPU (RTX 3060+)	Mid-sized models, well
8GB Mac / older laptops	Very small models, or not worth it

If your laptop is from 2023 or later with 16GB+ of memory, you can try local AI today.

OPEN-SOURCE AI, DECODED

It's not your chats made public. It's the *brain itself.*

A handful of models the big labs released for anyone to download and run — without a subscription, without sending data to a company.

MODEL	MADE BY	BEST FOR
Llama	Meta	General writing, brainstorming, summaries — the big one
Mistral	Mistral (FR)	Lightweight tasks; punches above its weight
Qwen	Alibaba	Coding and reasoning; strong on technical work
Gemma	Google	Small footprint, capable general use

> **Why they matter:** they can't train on your data — they're just a file on your hard drive. You control them. They keep working even if a company sunsets a product.
> The trade-off: not quite as capable as the latest GPT or Claude — but catching up fast, and more than enough for everyday writing.

WHAT I REACH FOR, WHEN

A small table I keep *in my head.*

YOUR SITUATION	WHAT I REACH FOR	*TIER*
Daily writing, brainstorming, social	ChatGPT or Claude, locked down	*2*
Drafting client emails	Claude Project with my voice file	*2*
Anything client-confidential	Claude desktop + Projects + discipline	*2*
Researching a public website	ChatGPT — no real privacy stakes	*1*
Anything regulated	Local AI: LM Studio + Llama / Mistral	*3*
Quick facts, recipes, questions	Any tool in default mode	*1*

Most of life lives in Tier 2. The honest answer to "is that safe enough?" is yes — done well, it's enough for the work most small business owners actually do.

THE "SHOULD AI DO THIS?" FILTER

Four questions I run *silently.*

1. Does this require human judgment? *A tone read, an apology, a hard "no."*
2. Does it involve someone else's private information?
3. Could a wrong answer hurt someone? *Medical, legal, financial.*
4. Would I be embarrassed if it leaked?

If the answer to any is yes — keep a human in the loop.

> *AI drafts. I decide what ships.*

IF YOU'VE ALREADY PASTED SOMETHING YOU WISH YOU HADN'T

Delete the chat. Flip the settings above. Use temporary chats from here on. Don't spiral — the risk is statistical, not personal. The rupture isn't the problem; the lack of repair is. You're not behind. You just weren't shown until now.

You can use AI seriously AND keep your work yours. The two things you needed to know are now in this letter — you'll know them for the rest of your life.

THE HONEST, PRACTICAL VERSION — EVERY WEEK

I write about AI for women, work, and family, *over on Substack.*

substack.com/@meganchristie1 →

Powerful and yours. More time. More confidence. More you.