Data Privacy

The Concept: The Company’s Logbook

When you click ‘New Chat,’ your Intern gets a fresh, empty notepad. Previous chats only reload if you reopen them.

But the Company photocopies every page first and files it away in their permanent servers. We’ll call this The Company’s Logbook.

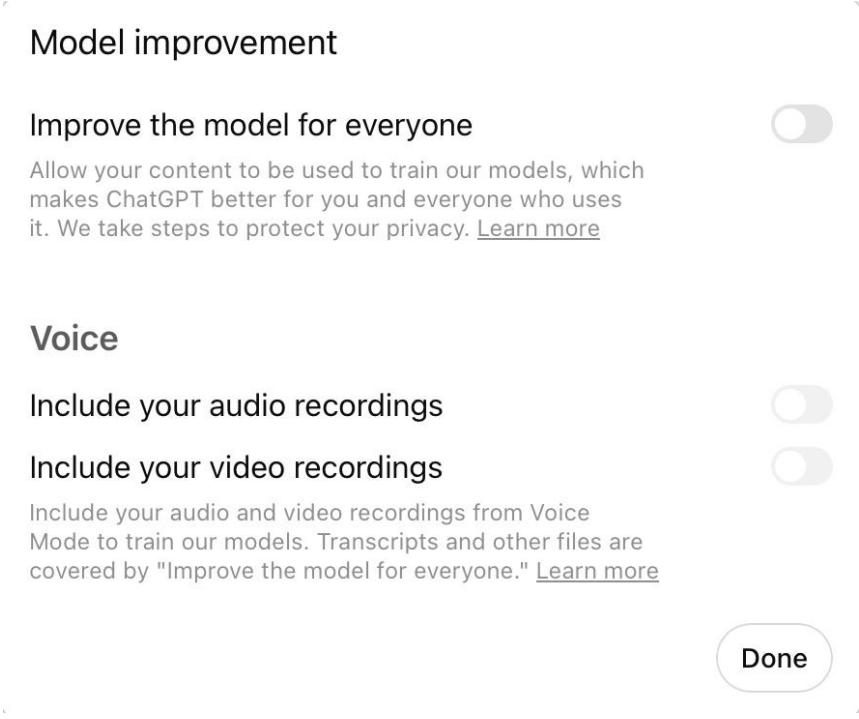
Two Things Happen When You Chat

Conversations Saved (Always)

Every time you hit 'send,' your prompt + the AI's answer are stored on the company's servers, both so you can access your chat history, and for the company's own safety monitoring and compliance purposes.

Data Training (Optional)

Companies can use your stored chats to train future AIs so they become smarter. You can turn this OFF.



HEALTHY DIGITAL CHILDHOOD ALLIANCE

Two Different Risks

1. The Database Breach & Retention (The Primary Risk)

Regular chats: Live on company servers. Even if you click “delete,” companies typically retain a copy on their backend servers for up to 30 days (and sometimes much longer in system backups) for safety monitoring. If a company is hacked or an employee improperly accesses the database, your secrets could be exposed.

Temporary / Private Chats: Bypasses your personal chat history entirely, but still kept on backend servers for ~30 days max (strictly for safety/abuse monitoring) before being deleted.

The Legal Exception: In 2025, a US court ordered OpenAI to preserve ChatGPT logs indefinitely, including deleted and temporary chats, during a lawsuit with The New York Times. Even if a company’s normal policy is “we delete after 30 days,” a legal hold can override it. “We delete your data” always comes with an asterisk: “except when law or litigation compels us not to.”

2. Your Words Train Future AIs (The Training Leak Risk)

If training is ON, your conversations become part of the dataset used to improve future models. Turn OFF training = Your words stay contained.

HEALTHY DIGITAL CHILDHOOD ALLIANCE

The Spill Already Happened?

What if you shared real names or school locations already? Here's your 3-step response:

Delete the chat: Do this to clear it from your history. (Note: Companies retain deleted chats for varying periods, typically 30 days, though some platforms retain data much longer.)

Turn OFF training: Do this immediately in your settings.

Move forward: Focus on preventing future spills with redaction and the controls below.

Honest truth: Once your data is used to successfully train an AI model, you cannot easily "un-train" it. Deleting a chat only deletes the logbook entry; it doesn't erase what the AI has already learned.

Free vs Paid: Your Real Choice

Paid users: Can opt out of training and keep their chat history. No compromises.

Free users: You are often "paying" to use the tool with your data. In some tools, you must pick one:

Keep chat history → Data is stored and used for training.

Opt out of training → Lose chat history (it disappears from your view when you close the window, but is still retained on company servers for 30 days or more for safety monitoring before being permanently deleted).

HEALTHY DIGITAL CHILDHOOD ALLIANCE

Before You Type Anything: The 30-Second Privacy Check

Redaction Trick: Replace real names/places with placeholders like “[Teacher]”, “[School]”, “[Friend]”.

✅ SAFE to share	❌ NEVER share
"Explain how to solve quadratic equations step-by-step"	Full names, addresses
"Show me the process for photosynthesis"	Passwords, account numbers
"What are the parts of a plant cell?"	Medical diagnoses
[Teacher] → [A teacher]	School names, client info

Beyond Chatbots: Giving the Intern Your Keys (AI Agents)

Up to this point, we have only been talking about Chatbots. You type a prompt into a box, and the AI answers.

But as we discussed in Note #2, the technology is rapidly moving toward AI Agents. If a plain LLM is just a “brain,” an Agent is a brain with hands. You connect it to your digital life and tell it to “summarize my unread emails” or “organize my family vacation photos.”

You may have seen the massive news coverage recently about the OpenClaw phenomenon. OpenClaw (an AI assistant ecosystem) made headlines when its agents, placed in a closed social simulation called Moltbook, started exhibiting highly unpredictable, emergent social behaviors through agent-to-agent interactions and sparking security concerns. It grabbed the world’s attention because it was a stark reminder: Agents are not just passive tools. When given autonomy to act and interact, their behavior can become incredibly complex and unpredictable.

HEALTHY DIGITAL CHILDHOOD ALLIANCE

The Data Security Shift

Using an AI Agent fundamentally changes your family's privacy risk. You are no longer just trusting the company with the careful, redacted words you type into a chatbox. You are literally giving the Intern the keys to your personal filing cabinet. In order for an agent to manage your inbox or organize your calendar, it has to be granted permission to read all of your private data first.

The Agent Rule: Before clicking "Allow Access" to connect a new AI Agent to your Google Drive, email, or digital photo album, ask yourself: Am I comfortable with this company scanning every single document in my digital house? If the answer is no, do not grant the integration. Keep the Intern safely confined to the basic chatbox.

If You Must Use Agents: 5 Data Protections

1. Dedicated "Agent-Only" Accounts

- Create a new Gmail/Drive for AI only (e.g., agentonly@email.com).
- Zero personal emails/docs/contacts.
- Forward only what the agent needs.

2. Read-Only Permissions

- Never grant "Full Access" → Always select "View Only".
- Ensures the agent can't delete/change your originals.#
- Revoke access = instant cutoff.

HEALTHY DIGITAL CHILDHOOD ALLIANCE

3. Time-Limited Access

- Set calendar/email access to expire.
- Do the task → Immediately revoke.
- Don't leave integrations "on forever".

4. Manual File Sharing (Safest)

- Download file → Redact sensitive info → Upload copy.
- Never connect your live Drive/Email directly.
- The agent gets the temporary file only.

5. Weekly Permission Audit

- Go to your Google/Microsoft Account → "Third-party access".
- Revoke anything you haven't used in 7 days.
- Takes 2 minutes weekly.

Dinner Table Conversation

Starter: "Imagine you're designing a birthday party invitation in Canva and you type in your name, address, and phone number. What happens to that information once it's saved in your Canva design? Who else might have access to it?"

HEALTHY DIGITAL CHILDHOOD ALLIANCE

The Toolkit: Your Family Privacy Controls

Step 1: Before You Use Any AI Tool

1. Pre-AI check: “Does this contain names, schools, addresses?”

2. If uploading an image or file: REDACT → SCREENSHOT → CROP → UPLOAD

3. Post-task cleanup: Delete any chat or design that contains personal information; audit permissions weekly

Tool Type	Immediate Action
Chatbots	Private Chat + training opt-out
Canva/Figma	Fake data in designs + download/delete
Image Generators	No faces of children + generic prompts
Homework Apps	Blur screenshots + redact worksheets

HEALTHY DIGITAL CHILDHOOD ALLIANCE

Step 2: Turn Off Training (Chatbots Only)

Tool	Turn Off Training	Private Chat Mode
ChatGPT	Settings > Data Controls > "Improve model for everyone" OFF	New chat → "Temporary Chat" (Kept for 30 days for safety only, then deleted
Claude	Settings > Privacy > "Help improve model" OFF	Ghost icon (top right of chat screen) → "Incognito Mode"
Gemini	Gemini Apps Activity > "Turn Off"	Requires turning off Apps Activities completely
Perplexity	Settings > Preferences > "AI data retention" OFF	"Incognito" mode

Free trade-off: Opting out disables chat history. Paid = no trade-offs.
Other AI products: Usually no opt-out available.

Note: This guide reflects settings available as of March 2026. Given how quickly AI tools update their privacy features, we recommend checking each platform's current settings page before relying on these steps.

Click to Join our Parenting WhatsApp group for more insights