

The Privacy Rules

What never goes into an AI chat, and the swaps that keep every prompt working anyway. You are allowed to use the tool. That is most of the point of this page.

If you would not read it out loud in a waiting room, it does not go in the chat.

That is the whole rule. Everything else here is the rule applied to the things that actually come up in a house, plus the substitution that keeps the answer as good as it would have been. Paranoia costs you the tool. Carelessness costs you something you cannot take back. A written rule means you stop re-deciding at eleven at night, which is when the re-deciding always goes badly.

What never goes in

Ten things. Read them once and you will recognize them for the rest of your life.

1 Full names of your kids

First name is usually fine. First plus last is a search result.

2 The school

Name, district, teacher's name, the classroom number on the form.

3 Your address

And anything that reconstructs it. The bus stop. The cross street. The photo of the mail.

4 Your employer

Your manager's name, and anything pulled out of a work system.

5 Dates of birth

Especially with a name attached. That pair opens accounts.

6 Medical detail tied to a person

Diagnoses, medications, therapist names, the portal message.

7 Money identifiers

Account numbers, the last four, insurance IDs, policy numbers.

8 Login information

Passwords, security answers, the code that just arrived by text.

9 Other people's private business

Your sister's divorce. The neighbor's diagnosis. It is not yours to paste.

10 Photos with any of it visible

The form with the letterhead. The screen with the tab open behind it.

What is actually fine

Your schedule, your routines, your meal rotation, the supply list with the school header cropped off, first names, ages, what your kids will and will not eat, your own opinions, the argument you had about the dishwasher, the shape of your week, your budget in round numbers, your grocery list, the text you are trying to write, how you actually feel about all of it.

That is nearly everything a household prompt needs. The rules cost you almost nothing in practice, which is the point of writing them down once. Worrying about the wrong half is how the tool quietly stops getting used.

The swaps

Every one keeps the answer exactly as useful. The model does not need the real noun. It needs the shape.

INSTEAD OF

WRITE

the kid's full name	my nine year old
the school name	her school
the teacher's name	her teacher
your street	our street, about fifteen minutes from her school
your employer	my job
a date of birth	she turns ten in March
a diagnosis	a standing medical thing we manage daily
a medication name	her morning medication
the doctor's practice	the pediatrician
an account number	the account

Two rules make the swaps work

Keep the shape, drop the identity. “My nine year old, who reads well and melts down when she is hungry” is a better input than a full name and nothing else. Specificity about behavior costs you nothing. Specificity about identity is the only thing that does.

Be consistent inside one chat. Call her “my nine year old” in message one and message forty. The moment you switch to a real name to clarify something, the whole conversation carries it.

Photos, which are the real leak

The camera is the fastest way into these tools and the easiest place to get careless, because a photo carries things you did not type.

Before you send a picture, look at the edges. School letterhead. A name in the corner. The address block on a form. A visible screen behind it. A prescription label. A calendar with a full name on the appointment.

Crop first. Cropping in your photos app is faster than re-thinking it after, and a cropped form answers the question exactly as well as the whole one.

The settings to go find

Do this once, today, in whichever tool you use.

Open the settings and look for the section about data, privacy, or training. There is a control over whether your conversations can be used to improve the model. Decide once and set it. There is usually a separate control for how long chat history is kept, and a way to delete conversations. Know where both are.

Menus move and the wording changes between tools and versions, so go look rather than trusting a screenshot from six months ago. Five minutes now, and you never think about it again.

For a genuinely sensitive one-off, use a temporary or incognito chat if your tool offers one, and close it when you are done.

Print it.

Run the swaps for one week and it stops being a decision you make at eleven at night. If this closed a tab, Out of My Head closes twelve. mainframemom.com/out-of-my-head