A FREE GUIDE BY MARYAM IDRIS

The Safe AI Guide

What to put into AI, and what to keep out.

AI saves time. It can write, explain, plan and create. And most of the best tools are free.

But what you put in matters. AI tools are very well-read assistants, with no loyalty to you and no promise that what you type stays private. That is why I teach one simple rule before anything else.

> *Imagine you are handing this to a very smart stranger on the street.*
>
> Would you tell them your business idea? Probably yes.
> Would you hand them your bank details? No.
>
> AI is that stranger. Useful. But not private.

What is inside

- The safe list and the leave-out list
- How to swap real details for safe ones, with examples
- Five questions to ask before you press send
- Settings to check in any AI tool
- What to do if you already shared something by mistake

I'm Maryam. I work in data and AI, and I build and use these tools every day. This guide is for anyone who wants to use AI with confidence, whether you are a student, a parent, a business owner or someone just starting out.

PART 1

The safe list and the leave-out list

If you are not sure which side something falls on, treat it as the leave-out list.

Safe to put in

- Business ideas you want to develop
- Content you want to create: captions, scripts, website text
- General questions, for research, learning and explanations
- Descriptions and prompts for images you want to generate
- Products and services you want to sell
- Public information that anyone could find online
- Your own work with the names and numbers removed

Keep out

- Your full name together with your address or ID details
- Bank details, card numbers, passwords and one-time codes
- Private photos of yourself or your family, especially children
- Confidential client or business information that is not yours to share
- Anything your employer or contract says is confidential
- Medical or legal information that could identify you or someone else
- Other people's private messages or details
- Anything you would not want a stranger to read

Photos, faces and voices

AI can create images, clone voices and make videos. Before you upload anyone's face or voice, ask yourself whether they have agreed. Never upload photos of children. When you share something AI-made, say that it is AI-made.

AI makes mistakes

AI can sound sure and still be wrong. Check facts that matter, and do not use it as your only source for medical, legal or money decisions. Use it to prepare your questions, then speak to a qualified person.

PART 2

Swap it, don't paste it

You can often get the help you need without the private details. Describe the situation. Don't paste the document.

DON'T

"Write an email to Amina Yusuf at 14 Rose Lane about her overdue invoice of £1,250."

DO

"Write a polite email to a customer about an overdue invoice. Keep it firm and kind. I'll add the details myself."

DON'T

Paste a client's contract and ask "Summarise this."

DO

"What clauses should I look for in a service contract, and what questions should I ask before signing?" Then read your own contract with that list.

DON'T

"Here are my bank statements. Help me budget."

DO

"Here are my rough monthly costs in categories: rent, food, transport, savings. Help me plan." Use ranges, not exact figures or account details.

DON'T

Upload a photo of your child to make a cartoon.

DO

Describe the character in words: "a smiling five-year-old girl in a yellow dress."

Three habits that help

- **Use roles, not names.** "Client A", "my manager", "a customer".
- **Use ranges, not exact numbers.** "About £1,000", not the amount.
- **Describe, don't paste.** Tell the AI what the document is about, then keep the original to yourself.

PART 3

Before you press send

1. **Could this identify me, or someone else?** A name, a number, an address, a face.
2. **Is it mine to share?** Client, employer and family information belongs to them.
3. **Would I be fine if a stranger read it?** If not, leave it out.
4. **Can I do without the detail?** Swap it for a role or a range.
5. **Am I about to rely on the answer for something important?** Check it with a person or a trusted source.

Settings to check in any AI tool

Every tool is different and the settings change, so check the current options in each one you use.

- **Training and history.** Look in the privacy settings for whether your chats can be used to improve the tool, and turn it off if you can. Many tools also have a temporary or private chat mode.
- **Delete what you no longer need.** Clear old chats, especially any that included real details.
- **Free versus paid.** Free versions can have fewer privacy options than paid or business versions. Read what the tool says it does with your data.
- **Keep work and personal separate.** Use different accounts, and follow your employer's AI rules.
- **Protect your account.** Use a strong, unique password and turn on two-step sign-in.

If you shared something by mistake

- Don't panic. Delete the chat and check the settings above.
- If it was a password or code, change it now.
- If it was bank or card information, contact your bank.
- If it was a client's or employer's information, tell them. It is better they hear it from you.

ONE LAST THING

Using AI in a small business?

If you run a business or a team, write a one-page AI rule and share it with everyone who works with you. Cover three things:

- **What is allowed:** for example, drafting posts, brainstorming and summarising public information.
- **What is not allowed:** customer details, payment information, passwords and anything confidential.
- **Who to ask:** one person people can go to when they are unsure.

The simple version

Share your ideas. Protect your people. Check what matters.

Stay in touch

I share what I'm learning and building on Instagram at **@iam_maryamidris**, and in my newsletter at **maryamidris.com**. If this helped you, send it to someone who is just starting with AI.

Maryam Idris · Founder, Quiet Systems and Data Habitat

This guide is general information and is not legal or professional advice. AI tools and their settings change often, so check each tool's current privacy options before you rely on them.