

Before You Paste Anything Into an AI Tool

- ☐ **Strip personal data first.** Remove names, email addresses, phone numbers, addresses and any data that identifies a real person. Replace with "Person A", "Company X" etc.
- ☐ **Remove financial specifics.** Exact salaries, bank details, account numbers, and card numbers should never go into a free AI tool. Use rounded or fictional numbers if the task allows.
- ☐ **Check for passwords and API keys.** Config files, .env files, and code snippets often contain credentials. Search for "password", "key", "token", "secret" before pasting.
- ☐ **Consider client confidentiality.** Would your client be comfortable seeing this data on someone else's screen? If not, anonymise or don't paste it.
- ☐ **Know your tool's training policy.** Free tiers of ChatGPT may use your inputs for training. Business/API tiers typically don't. Check the provider's data policy.
- ☐ **Use business-tier accounts.** Paid business plans (ChatGPT Team, Claude Pro, Gemini Business) offer data processing agreements and no-training guarantees.

Four Questions to Ask Any AI Vendor

- ☐ **1. Is my data used to train your models?** The answer should be "No" for any business plan. Get it in writing — a data processing agreement (DPA) or clear terms of service.
- ☐ **2. Where is my data stored, and for how long?** Know the country (UK GDPR applies if data leaves the UK) and the retention period. "Deleted after 30 days" is better than "retained indefinitely".
- ☐ **3. Who at your company can see my inputs?** Trust & safety teams may review flagged content. That's normal — but understand the scope.
- ☐ **4. Can I delete my data on request?** Under UK GDPR you have the right to erasure. A reputable vendor will have a process for this.

Consumer vs Business AI Tiers

Feature	Free / Consumer	Business / API
Data used for training?	Often yes (opt-out varies)	No (contractual guarantee)
Data Processing Agreement?	Rarely	Yes — request it
Audit logs?	No	Usually available
Data retention	Often indefinite	Defined period (e.g. 30 days)
SSO / access controls?	No	Yes

Your Four House Rules for Staff

Rule 1: Never paste personal data (names, emails, addresses, NI numbers) into any AI tool without anonymising first.

Rule 2: Use the company-approved AI tool and account — not a personal free-tier login.

Rule 3: Don't upload entire documents. Copy only the section you need — less data exposed = less risk.

Rule 4: If in doubt, ask. No one gets in trouble for checking first.

UK GDPR Basics for AI Use

- **You are the data controller.** If you paste customer data into an AI tool, you're responsible for what happens to it — not the AI vendor.
- **Lawful basis required.** You need a lawful basis (usually legitimate interest or consent) to process personal data via AI.
- **Record your processing.** Add AI tools to your Records of Processing Activities (ROPA).
- **Data minimisation:** Only share the minimum data needed for the task.
- **International transfers:** If the AI vendor stores data outside the UK, check they have adequate safeguards (UK adequacy decision or standard contractual clauses).