

Using AI safely with customer data: what to leave out and who checks

Most AI tasks don't need the private parts of a customer's email, and leaving them out costs nothing in quality.

Leave it out before you paste

- **PII** is information that can identify a specific person, alone or combined with other details.
- Never paste account and card numbers, Social Security and tax IDs, dates of birth, license numbers or health details.
- Drop full names or addresses the reply doesn't need. The test is not "no personal details ever", it is "only the details this reply needs".
- Write a short facts list yourself instead of pasting whole records.

Redact in three steps

1. Search the text for long numbers and @ signs before you paste.
2. Swap what you remove for clear placeholders like [CLIENT] or [ACCOUNT], so the AI knows something was removed.
3. Put the real details back in yourself, in your email app, after the AI step.

Settings that help, and their limits

Data controls

In ChatGPT's Settings, turn off **Improve the model for everyone** so chats on a personal account aren't used for training.

Training off

Doesn't mean private. Chats are still processed and stored to run the service.

Temporary Chat

Skips history and memory and isn't used for training. Turn it on before you paste. The data still goes to OpenAI.

People stay in charge

Human in the loop

A person reviews AI work before it reaches a customer. Make it structural, like an n8n Gmail tool set to **Draft** only.

AI use policy

Approved tools and plans, data that never goes in, allowed uses, and the review step before anything goes out.

Hiring notes

Score against job-related must-haves with a quote as evidence. Tell the AI: "Don't guess at age, family, health, religion or anything else that isn't job-related."

Remember: Send the AI only what the task needs, and have a person check the result before it reaches anyone. Your company's policy and industry rules come first.

Have a professional review it. This prompt helps you draft, not decide. AI can get the law wrong and doesn't know your jurisdiction or your facts, so have a licensed attorney review anything legal before you send or sign it.

Practice it free: Reply Faster: Turn a Messy Customer Email Thread into a Clear, Friendly Reply at learn.ynteractive.com/modules/chatgpt-reply-faster. This sheet: learn.ynteractive.com/content/cheat-sheets/ai-customer-data-safety. Businesses in the lesson examples are made up. By Robert Breen, October 1, 2026.