ChatGPT Part 9: Data Privacy, Security and Responsible Use

ChatGPT can save hours of work, but everything we type into it is data that must be handled with care. Responsible use rests on four habits: settings, sensitive information, checking, and policy. Each habit answers one simple question. In this part, Hadeel, an HR coordinator at a training company, shows how it works.

1. Settings

ChatGPT has data controls in its settings, where users can choose whether their conversations may be used to improve the models. The first question is: who may use what we type? OpenAI also offers temporary chats, which are not saved in the chat history and are not used to train its models. Business plans usually come with stronger privacy terms, so the plan we use matters. Because names and options change over time, we read the current help pages instead of relying on memory.

Example: A student opens ChatGPT to practise a job interview. She uses the Settings question: who may use what we type? She checks the data controls and starts a temporary chat, so her practice answers stay private.

At work: Hadeel wants ChatGPT to help rewrite a training course outline. She uses the Settings question: who may use what we type? She checks the data controls in her company account and confirms which plan the company pays for before she starts.

2. Sensitive

Some information should never enter a public AI tool, because we cannot take it back once it is shared. The question is: would we share this text with strangers? That includes passwords, customer and employee details, health records, contracts, and plans that are not yet public. When we still need help with such text, we remove names and numbers or replace them with simple labels. A short rule of thumb is: if it would hurt to see it outside the company, it should not be pasted.

Example: A neighbour wants help writing a complaint about a landlord. She uses the Sensitive question: would we share this text with strangers? She removes the address and the phone number before asking for the wording.

At work: Hadeel needs a summary of an employee's performance review. She uses the Sensitive question: would we share this text with strangers? The review contains private details, so she keeps it out of ChatGPT and writes the summary herself.

This document is a property of Asaseeyat Academy - © Copy Right Protected.

3. Check

ChatGPT can make mistakes, and its answers can reflect bias from the data it learned from. The question is: is it accurate, fair, and safe to reuse? We verify facts and numbers, look for stereotypes or missing viewpoints, and make sure we are not copying protected work. Copyright rules differ between countries and companies, so for published material we follow our company's guidance. Treating the answer as a first draft keeps the responsibility with us.

Example: A teacher asks ChatGPT for a history summary for her class. She uses the Check question: is it accurate, fair, and safe to reuse? She compares the dates with the textbook and corrects one wrong year.

At work: Hadeel asks ChatGPT for a job advert. She uses the Check question: is it accurate, fair, and safe to reuse? She finds a phrase that favours one group and rewrites it, and she confirms that no text was copied from another company's advert.

4. Policy

A company AI policy explains which tools are approved, what data may be used, and who must review the results. The question is: what does our policy allow, and who reviews the work? When a policy exists, we follow it, and when it does not, we ask a manager before using AI for client work. Important decisions about people, such as hiring or discipline, should always include human review. Together, these rules keep the benefits of AI and reduce its risks.

Example: A volunteer group asks whether it may use ChatGPT for donor letters. It uses the Policy question: what does our policy allow, and who reviews the work? The coordinator reads the group's rules, and a second volunteer reviews each letter.

At work: Hadeel's company policy allows ChatGPT for drafts but not for client data. She uses the Policy question: what does our policy allow, and who reviews the work? She drafts with it, a colleague reviews the result, and a manager approves the final version.

Conclusion

In summary, safe use of ChatGPT is built on four habits. We control our settings, protect sensitive information, check every answer, and follow the company policy with human review. Before every prompt, the key question is simple: would we be comfortable if this text were seen outside the company?

Sources

- OpenAI Help Center: Data Controls FAQ – https://help.openai.com/en/articles/7730893-data-controls-faq
- OpenAI: Enterprise privacy at OpenAI – https://openai.com/enterprise-privacy/
- OpenAI: Usage policies – https://openai.com/policies/usage-policies/

- ChatGPT and OpenAI are trademarks of OpenAI. This video is independent training material and is not affiliated with OpenAI.

This document is a property of Asaseeyat Academy - © Copy Right Protected.