



Using AI Safely: What to Share and What to Check

Practical examples to help you protect private details and check an answer.

Before You Start

Use a general example. Leave private details out.

Leave Out Private Details

Check the Source

Decide Yourself

- 1 Start with a general question: Try 'Explain Wi-Fi in plain language' or 'Draft a friendly thank-you note.' You do not need to include names, addresses, or account details.
- 2 Replace private details: Say 'my relative' instead of a full name. Never paste passwords, sign-in codes, bank details, medical records, or private client documents into a public AI chat.
- 3 Look before you upload: A photo or screenshot may show messages, account numbers, or an address. Remove private details first. Check the tool's privacy and sharing settings.
- 4 Check the answer yourself: Ask for a source, then open the original website and confirm it supports the claim. Check dates and numbers. A confident answer or a link is not proof.
- 5 Keep the final decision: Read a draft before sending it. Ask a qualified person about high-stakes decisions. If you are unsure what a tool will share or change, pause before continuing.

Official Resources: NCSC: AI and cyber security

When to Ask for Help: Before uploading private material, connecting accounts, or acting on an answer you cannot verify.

Questions You Can Ask: Can I ask this without identifying anyone? · Does the original source support this answer?

NOTES TO KEEP NEARBY
