

Before You Put That Into AI.

A quick check before you paste, upload or share information with an AI tool.

AI can make it incredibly easy to work with information.

Paste in some notes. Upload a document. Summarise a report. Analyse a spreadsheet.

But before you do, take a moment to think about what you're sharing, which tool you're sharing it with and whether it should be there at all.

1. What information am I about to share?

Take a look before you paste or upload it.

Does it contain:

- names, email addresses, phone numbers or other personal information?
- information about beneficiaries or service users?
- health or disability information?
- safeguarding information?
- HR, employment or recruitment information?
- financial or payment information?
- passwords, login details or security information?
- confidential organisational information?
- information somebody has shared with you privately?
- anything else that could cause harm or embarrassment if it were handled incorrectly?

If yes, don't automatically put it into AI.

Stop and check first.

2. Is this an AI tool my organisation has approved?

Using AI “for work” doesn't necessarily mean you're using an organisation-approved system.

Your organisation may have specific versions of tools such as Microsoft Copilot, Google Gemini or ChatGPT that have been configured or purchased for work.

A free personal account may have different terms, settings and protections.

Ask:

Am I using the right tool and account for this information?

If you don't know, find out before sharing anything sensitive.

3. Do I know what happens to the information?

Different AI products, accounts and settings can handle information differently.

Before using sensitive or confidential information, you may need to understand things such as:

- whether prompts or files are retained
- whether information can be used to improve or train models
- who can access it
- how long it is kept
- whether it can be deleted
- where information is processed or stored
- what contractual or organisational protections apply

Don't assume all AI tools work the same way.

And don't rely on the AI chatbot itself to tell you what its privacy terms are. Check the provider's current documentation and your organisation's guidance.

4. Do I actually need to share all of this?

Often, you don't.

Ask yourself:

What is the minimum information the AI needs to help me?

Could you:

- remove names?

- remove identifying details?
- summarise the situation instead of uploading the original document?
- use fictional or dummy information?
- provide only the relevant section?
- describe the structure of the data rather than sharing the data itself?

Reducing the information you share can reduce the risk.

But remember: removing someone's name doesn't necessarily make information anonymous. Other details may still identify them.

5. Is this particularly sensitive?

Some information deserves an extra stop.

Be especially cautious with information involving:

- children and young people
- safeguarding
- health
- disability
- sexuality or gender identity
- racial or ethnic origin
- religion
- criminal allegations or convictions
- immigration status
- people's finances
- complaints or investigations
- employment disputes

If you're unsure whether the information is appropriate for the AI system you're using, don't guess. Check.

6. Would the person reasonably expect their information to be used this way?

Just because your organisation holds information doesn't automatically mean every use of it is appropriate.

Think about:

- why the information was originally collected
- what the person was told

- what you're now asking AI to do with it
- whether this is consistent with your organisation's policies and responsibilities

This matters particularly when people have trusted your organisation with sensitive information.

7. What am I asking the AI to do with it?

Risk isn't only about the information you put in.

It's also about what you're asking the system to do.

There's a big difference between using an approved tool to help format an internal document and asking AI to assess somebody's suitability for a job, interpret a safeguarding concern or recommend whether somebody should receive a service.

The more a use could affect someone's rights, opportunities, safety or access to support, the more careful you need to be.

8. What will I do with the answer?

Before sharing the information, think one step ahead.

Will the AI output be used to:

- inform a decision?
- communicate with somebody?
- go into a case record?
- appear in a report?
- be published?
- influence how somebody is treated?

If the consequences of getting it wrong are significant, the checking and human oversight need to be stronger too.

The 10-second check.

Before you paste or upload something, ask:

WHAT is in it? Is there personal, confidential or sensitive information?

WHERE is it going? Is this an approved tool and account, and do I understand how it handles information?

WHY am I sharing it? Does the AI actually need this information to do the task?

WHAT HAPPENS NEXT? Could the output affect somebody or be relied upon for something important?

If you're not comfortable with the answer to any of those questions:

Stop. Check. Then decide.

You don't have to work it out alone.

Your organisation should give staff clear guidance about which AI tools can be used, what information can be shared with them and where to go when you're unsure.

If that guidance doesn't exist yet, that's an organisational governance issue, not something individual staff should be expected to solve on their own.

For a wider look at your organisation's approach, try the free AI for Non-Profits Governance Checker.