BOURNEMOUTH
UNIVERSITY

Think before you ask: Privacy risks when using AI tools

Artificial intelligence (AI) tools such as chatbots, image generators, and writing assistants are now widely available and easy to use. While they can be helpful, they also carry real privacy risks. What you choose to type into or upload to an AI system can have consequences for you and for others. This guidance explains what those risks are and how to use AI tools more responsibly.

Why privacy matters with AI

Many AI tools are provided by third-party companies. When you use them, your inputs may be stored on external servers, used to improve or train future AI systems, accessed by people outside your organisation, or subject to laws and practices you cannot see or control. Once information is shared with an AI tool, you may lose control over it.

What counts as personal or sensitive data?

Before using AI, pause to consider whether what you're sharing includes personal data about yourself or others (such as names, contact details, or student/staff IDs), confidential work information, or sensitive personal data (like health, wellbeing, disciplinary matters, or safeguarding concerns). Drafts of assessments, feedback, or internal documents, as well as data about children or vulnerable people, also require extra care. If the information relates to a real person, especially someone else it deserves special attention.

Key privacy risks to be aware of

Some risks are especially important to keep in mind:

1. **You cannot assume confidentiality.** Most public AI tools are not private spaces. Treat them as if you were posting on a public forum.
2. **Information may be reused.** Some AI providers use submitted data to improve their systems. Even if names are removed, details may still be recognisable.
3. **Data can be stored outside the UK.** This can create legal and ethical issues, particularly for organisations that must follow data protection laws.
4. **You are responsible for what you share.** Uploading someone else's data without consent, even "just to see what the AI says" can still be a breach of trust or policy.

Think before you ask: A simple pause

Before typing a prompt or uploading a file, pause and ask yourself: Would I be comfortable sharing this information with a stranger? Does this include data about another person? Is there a way to ask the question without including personal or identifiable details? Would I be happy if this information was stored or reused? If you have any doubts, it's best not to upload the information.

Safer ways to use AI

You can still use AI tools more safely by:

- Keeping prompts general and anonymous
- Removing names, dates, IDs, and unique details
- Using fictional or clearly hypothetical examples
- Asking for help with structure, ideas, or explanations—not real data
- Using approved, organisation-provided AI tools where available

A shared responsibility

Responsible AI use protects not just you, but your colleagues, students, and community. Privacy is not only a legal requirement—it is about respect, trust, and care for others. Using AI thoughtfully means recognising that convenience should never come at the cost of someone else's data or dignity.