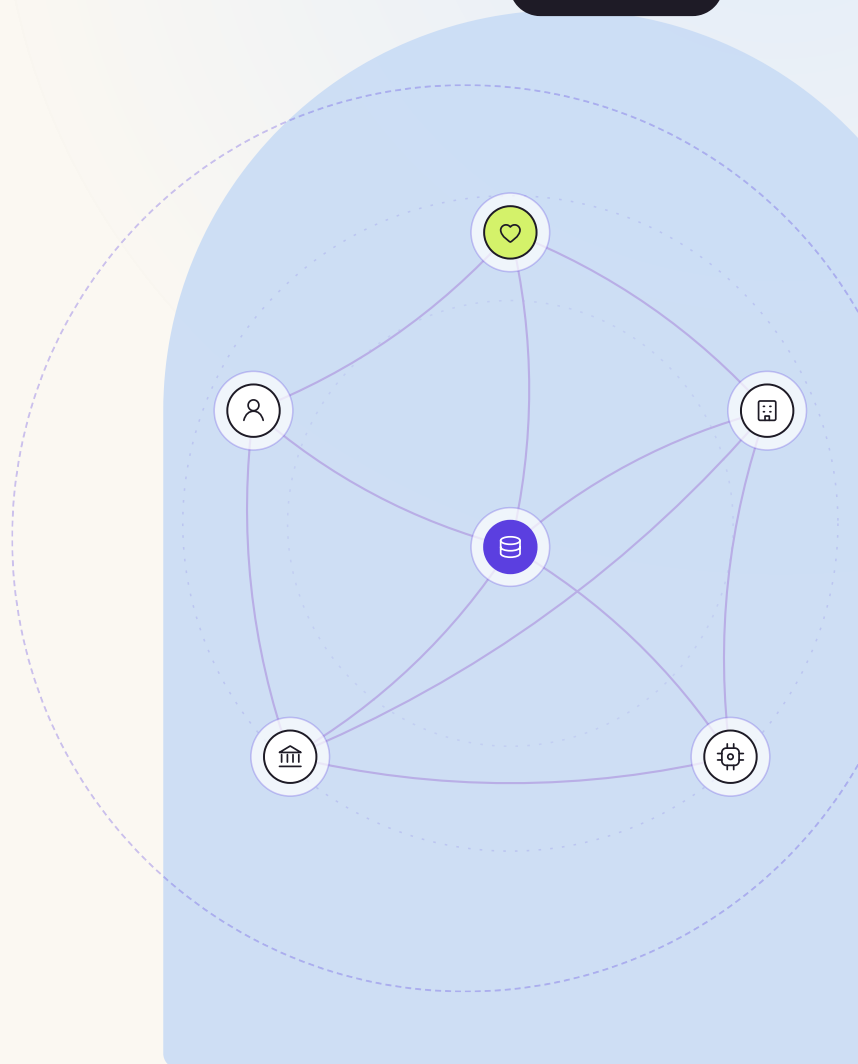




 QUESTION SET · AI REGULATION & GOVERNANCE

Questions to ask before staff use a generative AI tool

Fourteen questions to answer before a chatbot, writing assistant or other generative AI product is used with work information.

Generative AI tools are easy to sign up for and easy to paste information into. That is the risk. In October 2024 the Office of the Australian Information Commissioner (OAIC) published guidance on privacy and the use of commercially available AI products. It makes a simple point: privacy obligations apply to any personal information put into an AI system, and to any output that contains personal information.

The OAIC also says AI products should not be used simply because they are available, and that due diligence is ongoing, not “set and forget”. As a matter of best practice, it recommends that organisations do not enter personal information, and particularly sensitive information, into publicly available AI chatbots.

The questions below help you decide whether a tool is suitable before staff start using it. Answer them for each tool, and for each significant way it will be used. If you cannot answer a question, treat that as a finding.

The information going in

1. **What information will staff enter?** Be specific: public material, internal documents, client files, customer records, staff records. Personal information and sensitive information (such as health information) need the most care.
2. **Is that information needed for the task?** The OAIC encourages minimising the personal information entered into AI systems. Ask whether the task can be done with de-identified or summarised information instead.
3. **Was the information collected for a purpose that covers this use?** Under Australian Privacy Principle (APP) 6, personal information is generally used or disclosed only for the purpose it was collected for, unless an exception applies, such as consent or a related secondary purpose the person would reasonably expect.

Retention and training

4. **Does the provider keep what we enter, and for how long?** Read the service terms and privacy documentation for the account type you will actually use. Consumer and business accounts often differ.
5. **Can the provider use our inputs or outputs to train or improve its models?** The OAIC notes that training use can create a risk of personal information resurfacing for other users. Find out whether this is on by default and whether it can be switched off.
6. **Can we delete information once it has been entered?** The OAIC warns that information entered into some tools may be impossible to remove.

Location and access

7. **Where is the information processed and stored?** If it leaves Australia, APP 8 on cross-border disclosure may be relevant.
8. **Who can see it?** Ask whether the provider's staff or third parties can access inputs or outputs, and in what circumstances. Entering information into a tool may be a use or a disclosure under the APPs depending on whether it stays within your effective control.
9. **What security protections apply?** APP 11 requires reasonable steps to protect personal information. Ask about the provider's security controls, its security history, and how your own accounts and access are managed.

Accuracy and human review

0. **What is the tool good at, and what are its known limitations?** The OAIC notes that AI systems are known to produce inaccurate or false results. Check whether the tool has been tested for your intended use.
1. **Who checks the output before it is relied on?** APP 10 requires reasonable steps to ensure personal information is accurate, up to date and complete. Decide who reviews AI output, and for which tasks review is mandatory.
2. **Could the tool create new personal information about someone?** The OAIC treats personal information that AI generates or infers as a collection, which must meet the APP 3 requirements.

Transparency and governance

3. **Will people know AI is involved?** The OAIC recommends updating privacy policies and notices with clear information about AI use, and clearly identifying public-facing AI tools such as chatbots.
4. **Who approved this tool, and who owns it?** Record who decided the tool is suitable, what it is approved for, what staff must not enter, and when the decision will be reviewed. Staff need to be told these rules in plain language.

How to use the answers

If the answer is...	It usually means...
Clear and acceptable	The tool may suit the stated use, with the controls you identified
Unclear	More due diligence is needed before staff use it with work information

If the answer is...	It usually means...
Unacceptable	The tool, the account type or the intended use needs to change

Keep the answers. They form part of the record of how your organisation decided to use AI, and they will need revisiting when the tool, its terms or your use of it changes.

Next step

These questions show where a single tool stands. Lexora's AI Governance Readiness Assessment looks at how your organisation selects, approves and oversees AI tools as a whole.

General information, not legal advice. It does not cover every obligation that may apply to your organisation, and you should obtain legal advice on your specific circumstances.

Sources

1. OAIC, Guidance on privacy and the use of commercially available AI products (October 2024)
<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products>



Better governance. *Greater confidence.*

Lexora is an Australian-first advisory business. We help organisations understand their privacy, data and AI obligations, assess risk, build governance frameworks and put practical controls in place.

OUR PRACTICES

Privacy & Data Protection

AI Governance & Responsible AI

Data Governance

Regulatory Readiness & Compliance

WAYS TO START

Privacy Health Check

AI Governance Readiness Assessment

Data Governance Review

Regulatory Readiness Consultation

DISCUSS YOUR GOVERNANCE NEEDS

lexoraai.com.au

info@lexoraai.com.au

More free guides: lexoraai.com.au/resources

This guide is general information, current at the date shown. It is not legal advice and does not take account of your circumstances. Lexora is not a law firm. Check the primary sources before relying on any date or requirement. © 2026 Lexora. You are welcome to share this guide unaltered, with this page attached.