Privacy Commissioner
Te Mana Mātāpono Matatapu

Artificial Intelligence & Privacy: What you need to know.

Thinking about privacy is vital if you are going to use artificial intelligence (AI) tools well.

Privacy is a starting point for responsible use of AI tools

AI refers to computer systems that do tasks which seem like intelligent behaviour, such as finding patterns or categorising. This includes generative AI tools, as well as other systems that interpret data or automate tasks. We want to make it easy for you to know the potential privacy risks associated with AI and what our expectations are.

Our starting point is that the Privacy Act applies to everyone using AI tools in New Zealand. The Information Privacy Principles (IPPs) set out legal requirements on how you collect, use, and share personal information. Before using these tools, you need to understand enough about how they work to be confident you are upholding the IPPs. The best way to do this is to do a Privacy Impact Assessment (PIA) before you start, and to update it regularly.

You need to consider the information privacy principles when using AI tools

When working with personal information, the IPPs set requirements around how you collect it (IPPs 1-4), how you use and protect it (IPPs 5-10), and how you share it (IPPs 11-12). There are also specific requirements on unique identifiers (IPP13). The IPPs apply to each stage of building and using AI tools, from **collecting training data**, to **training** a model, **taking user input**, receiving a **response**, and **taking action** as a result. Key questions to ask include:

- **Is the training data behind an AI tool relevant, reliable, and ethical?** AI tools reproduce patterns from their training data. This may include personal information collected in ways that breach IPPs 1-4. Gaps or biases may limit accuracy (IPP8).
- **What was the purpose for collecting personal information? Is your use related?** You need to be confident you are using personal information in ways that fit the purpose for which it was collected. Reusing information for training may go against this (IPP10).
- **How are you keeping track of the information you collect and use with AI tools?** You need processes for access and correction if people request that (IPP6,7).
- **How are you testing that AI tools are accurate and fair for your intended purpose? Are you talking with people and communities with an interest in these issues?** Doing a good Privacy Impact Assessment may require engaging with the community, including Māori, to help you understand and uphold fairness and accuracy (IPP8).
- **What are you doing to track and manage new risks to information from AI tools?** You must keep personal information secure, including prompts and training data (IPP5).

If in doubt, we recommend you do not use AI tools to handle personal information.

Thinking about privacy will help you understand AI tools better

We all rely on people and organisations taking responsibility for their actions in context. There is a lot of concern about AI tools creating new risks for privacy, trust, and accountability. Proactively thinking about privacy will help you use these tools better and manage risk.

You can find out more information on OPC's website at www.privacy.org.nz. If you would like to talk with us about this work, please email us at ai@privacy.org.nz