Fact Sheet May 2026

Engaging with Artificial Intelligence

Who is this information for?	Members of the public seeking information about AI and the privacy issues associated with it.
Why is this information important to them?	It is intended to assist in understanding how AI involves privacy and can impact the security of personal information.

What is AI?

Artificial intelligence (AI) is a type of computer technology that can perform complex tasks that used to require human intelligence to complete. This technology allows machines to think, learn, create, reason, recognise patterns, make decisions, or solve problems.[1]

AI is not a single tool or system, it is an entire ecosystem made up of ideas, methods, and technologies that work together. These include machine learning, deep learning, neural networks, natural language processing, computer vision, and more. Together, they allow machines to interpret the world, understand data, and respond in intelligent ways.

What are some types of AI?

Artificial intelligence comes in several forms, each defined by its capabilities and the ways it can support and improve efficiency, service delivery or problem solving. Different types of AI are designed to analyse data, recognise patterns, perform tasks automatically, or send information to and from the correct device at the right time.

There are many categories of AI, but some of the main types include Generative AI, Agentic AI, Predictive AI, Traditional AI, and Narrow AI. These systems work quietly in the background of our digital tools, supporting our daily activities.

AI can appear in everyday tools, apps, and systems, often without us even realising or noticing it. Some common examples include:

- **Chatbots** – help answer questions, provide customer support, or automate conversations.
- **Photo filters** – recognise faces and objects to apply effects automatically.
- **Voice assistants** – such as Siri, Alexa, or Google Assistant, which can understand and respond to spoken commands.
- **Face recognition** – used to unlock phones or identify people in photos.
- **Self-driving cars** – use cameras, sensors, and AI algorithms to detect surroundings and make driving decisions.

These are some examples that show how AI is integrated into modern technology.

Does understanding AI matter?

Yes. Understanding AI has become increasingly important because it is no longer a futuristic idea. AI is already here and is rapidly evolving and becoming increasingly embedded in our everyday lives. Gaining awareness and understanding of how AI works helps individuals to make informed choices, protect their personal information, and recognise potential risks. It also helps people understand the benefits AI offers, how it improves efficiency, and the responsibilities involved in using these technologies safely, ethically and responsibly.

How does AI affect privacy?

AI tools are data driven and rely on large data sets which often include personal information which can create new privacy risks or amplify existing privacy risks. AI affects privacy when it depends on collecting, analysing, and learning from large volumes of personal data. As these systems process information, they can uncover details about individuals, shape decisions made about them or create risks if the data is not managed securely.

Many of the products, devices, and networks people use daily include AI-driven features. In some situations, the personal information gathered through these systems can be leveraged by businesses for marketing insights, targeted advertising, or even sold to other companies.

[1] See Digital NSW: A common understanding: simplified AI definitions from leading standards

What are the risks in using AI?

While AI can be a useful tool, AI is not without limitations. It can cause inaccurate and biased results, provide incorrect results or spread disinformation. It is also capable of creating vulnerabilities through fake digital images, videos or audio clips by generating but convincing fabricated content.

How can I protect my personal information when using AI?

You can protect your personal information when using AI by being mindful of what data you share, understanding how that data is used, and adjusting the privacy settings available to you.

Individuals and agencies can take several practical steps to safeguard privacy and personal information, including:

- **Limiting the amount of personal information you provide.** Avoid entering sensitive details, such as your full name, home address, phone number, financial information, health records, or identification numbers into AI tools unless you fully trust the service and understand how your data will be managed. Treat AI as a public forum.
- **Read and understand privacy policies and terms of use.** Review the Privacy Policy, Terms and Conditions, and any data-handling documents associated with the AI tool. If the policies do not clearly protect your data or raise concerns, consider avoiding the service entirely.
- **Review and adjust privacy settings**. Where possible, disable features that store or share your chat history or interactions. Opt-out of unnecessary data collection or sharing options. Disable any training or logging features. Proactively delete your conversation logs.
- **Use trusted and secure platforms.** Choose AI tools provided by reputable organisations and avoid fake apps or phishing websites that attempt to collect personal information.
- **Use secure network connections.** Avoid using AI tools that require personal or sensitive information while connected to unsecured public Wi-Fi networks, as these can expose your data to security risks.
- **Keep devices and software up to date.** Regular software updates include important security improvements that help protect your information and devices from vulnerabilities.
- **Use strong passwords and multi-factor authentication.** Create unique passwords for accounts linked to AI tools and enable multi-factor authentication to reduce the risk of unauthorised access.
- **Be alert to new features in applications and services.** Social platforms, websites and applications are increasingly integrating AI chat features or AI-powered recommendations into their tools. Be mindful that these services may be collecting your data, potentially sharing it with third parties. Details of these changes should be included in privacy policies and terms of use.

What should I do if I've already shared too much personal information with an AI tool?

If you think you've provided more personal information to an AI tool than you intended, there are several steps you can take to reduce potential risks and protect your privacy moving forward:

- **Stop sharing information immediately.** Avoid supplying any further personal, sensitive, or identifiable details to the tool.
- **Review the tool's privacy settings.** Check whether you can delete previous chat history, turn off data collection, or disable the tool from using your information for training or other purposes.
- **Update important credentials.** If you shared login details, addresses, or other sensitive information, change your passwords immediately and update any accounts or credentials that may now be at risk.
- **Monitor your email, banking, and other important accounts.** Check for any unusual activity. If anything looks suspicious, act quickly to secure the account.
- **Contact the organisation if necessary.** If the AI tool is operated by a company or government agency, you can contact their privacy team to and request deletion and raise any concerns

Thinking of Using AI to contact agencies?

It can be appealing to use AI to help us to write emails or correspondence or when you need information to contact or engage with an agency. It can seem like a faster and easier way.

However, AI generated content can contain errors, omissions or incorrect or unreliable information. It's important to remember that AI generates information based on patterns, what data it has been trained on and generally summarises information.

It's possible that using AI might refer you to information, laws or cases that the AI thinks will be helpful but which are not necessarily correct. There are many reported examples now of where AI has referenced cases or laws which don't exist.

Understanding and being aware of the limitations of AI when interacting with agencies will assist with ensuring

that you are not working with wrong information. While AI is a tool, it can make mistakes and outputs may not always be accurate or complete.

Always check the information that has been provided before relying on it. Take the time to search the case or law it refers you to before relying on it.

You should take the time to refer to the relevant agency's website or other sources of information especially if AI is the only source for the information. Agencies publish a broad range of material on their role, work and functions which can help you in your interactions with them.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.

The development of this fact sheet was informed by guidance developed by the Office of the Privacy Commissioner for Personal Data, Hong Kong.