



Policy on Use of Artificial Intelligence (AI)

Policy statement

Emerging technologies provide CMCNZ staff with the opportunity to improve efficiency in everyday tasks, as well as providing improved outputs for our stakeholders. Many emerging technologies that could be used by staff incorporate AI.

If AI is used, there are specific processes and checks that will be necessary to ensure the work is accurate, we maintain the standards of work that stakeholders expect, as well as ensuring that we protect ourselves and stakeholders from any threats of data or privacy breaches.

The Council has implemented this policy to establish guidelines for the responsible use, development, and governance of Artificial Intelligence (AI).

Key principles

- **Transparency:** AI systems should be designed and implemented with clear documentation on how decisions are made.
- **Fairness:** AI must not discriminate or reinforce bias.
- **Privacy and security:** AI must comply with the data protection laws (and the Privacy Act 2020) and ensure user data security. Sensitive discussions should not be processed by AI unless authorised and staff must ensure that privacy (and specifically the obligations under the Privacy Act 2020), ethics and human rights are safeguarded.
- **Accountability and consent:** Users and developers must take responsibility for AI outputs and ensure continuous monitoring. If AI tools record or process meeting content, the content must be scrutinised to ensure it reflects the meeting accurately. Consent to record a meeting is required.
- **Disclosure:** Participants must disclose if they are using AI tools to transcribe, summarise, or assist in discussions. AI-generated responses or insights must be clearly identified to avoid confusion between AI and human contributions. AI insights should be scrutinised using available citations.
- **Human oversight:** AI should assist rather than replace human judgment and humans must retain the accountability of the oversight of any information generated by AI. Staff are to retain human oversight in the use of AI, including verifying the accuracy of the information.

Acceptable use

AI technologies should be used to enhance productivity, improve user experiences, and drive innovation while adhering to ethical standards.

AI technologies should be considered when holding online meetings and an external participant is clearly using AI to note take or record your session.

Misuse, including malicious automation or deception, is strictly prohibited.

Acceptable AI tools

The following outlines the current AI tools that have been approved for use in specific use cases by staff. No other AI tools should be used without prior review for their compliance with this and other policies.

To gain access to existing approved AI tools, or to request a new tool be reviewed for suitability and compliance with our policies, please speak with the Registrar.

The Council has approved the following specific AI tools:

- **Microsoft Copilot:** This AI assistant is integrated into Microsoft 365 apps like Word, Excel, PowerPoint, Outlook and Teams, making it a versatile tool for various work-related needs.

As an AI assistance tool offering numerous benefits by automating tasks, boosting productivity, and enabling users to focus on strategic work, Copilot can assist with various tasks, including writing, summarising, creating images, and even generating code.

Within the current setup, personal information entered in Copilot is not shared with other AI systems or the broader public. Microsoft's 365 Copilot is designed to keep your interactions private within the Microsoft 365 service boundary.

- **Adobe Suite:** is actively integrating AI across its product suite, with a focus on generative AI, particularly through its Adobe Firefly product. This includes features like AI Assistant in Adobe Acrobat and enhancements in Photoshop and Illustrator.

Generative AI is a form of artificial intelligence that creates new content — like text, images, video, audio and computer code — based on patterns it learns from existing data. Adobe encrypts and stores PDF content, user queries, and responses in a cache for 12 hours and then all content is automatically deleted after 12 hours.

- **External user AI tools:** Often attendees of hosted meetings will now have an AI tool on their device. For example, notetaker.ai, fireflies.ai, otter.ai. The Council will not block these attendees from the use of AI on their own devices, however, advise staff to be consciously aware of this in all meetings.

Third-party AI tools (e.g. ChatGPT, Otter.ai, Notetaker.ai, Fireflies.ai, OpenAI) are unauthorised in our toolkit for multiple reasons. While impressive, they can have limitations and drawbacks that might make it unsuitable for certain

tasks or contexts. Their responses are based on patterns, not facts, and can be inaccurate or biased. More importantly, as it is a cloud-based third-party system hosted outside of Aotearoa New Zealand, it cannot guarantee:

- Where data is stored or processed
- Who has access to that data
- Whether Māori data sovereignty principles are upheld.

Unapproved or unauthorised AI tools and applications must not be used.

For all types of AI:

- **Request access to an AI tool before it is used:** Before its use, staff must submit a formal request for any new AI tool to the Registrar. This will then be presented to the Council and the decision about the tool will be made. The Registrar will communicate the final decision to staff as required.
 - **Understand the security features of the tool before using it:** This includes reviewing the tool's terms of service, and privacy policy. DTSL will be best placed to support this.
 - **Protect confidential and personal data:** Staff must not upload or share any data that is confidential, proprietary, or protected by regulation without prior approval from the Registrar. This includes data related to practitioners, staff, or stakeholders.
 - **Maintain data privacy:** Staff must exercise discretion when using personal information in public AI tools. If the AI tool is publicly hosted, staff should ask themselves the question, "Would I be comfortable sharing this information outside of the Council?" before uploading or sharing any data into AI tools.
 - **Control access:** Staff must not give access to AI tools to other staff or people outside the Council. Speak to the Registrar to grant access to someone that fits this description.
 - **Comply with existing security policies:** Staff must apply the same security best practices we use for all Council data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies.
 - **Confirm accuracy of information** – check and double check the content before using outputs for decision-making or external use. This includes verifying all references.
 - **Check for completeness** – some AI tools are only trained up to a certain date, so ensure there are no recent gaps that need to be filled before using AI generated content for decision-making or for external use.
-

Training and awareness	Staff must be trained on AI best practices to ensure responsible use and mitigate risks.
Privacy, reporting and accountability	The Council is committed to protecting the privacy of individuals and complying with the obligations of the Privacy Act 2020. AI usage, such as undisclosed AI involvement or potential data security risks, or any concerns about AI misuse should be reported immediately to the Registrar.
Policy approved	September 2025
Review	Given the nature of the technology industry and the speed in which new AI is being introduced to the public domain, this policy is a living document. This policy will be reviewed periodically to ensure it continues to meet our safety needs and complies with relevant legal and regulatory requirements.
Acknowledgment	The Council would like to acknowledge the Nursing Council of New Zealand for their assistance in developing this policy.