



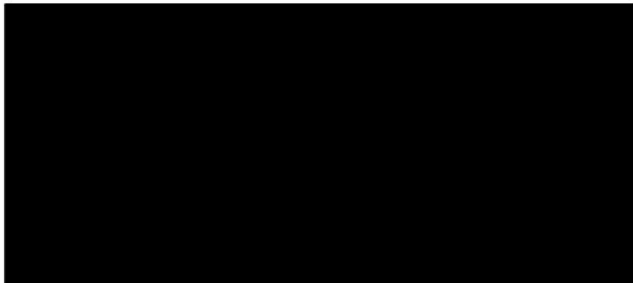
Ref: [REDACTED]

Civic House, 110 Trafalgar Street
PO Box 645, Nelson 7040, New Zealand

P (03) 546 0200

E LGOIMA@ncc.govt.nz
[nelson.govt.nz](mailto:LGOIMA@ncc.govt.nz)

22 July 2025



OFFICIAL INFORMATION REQUEST FOR USE OF GENERATIVE AI BY COUNCIL STAFF

I refer to your official information request dated 25 June 2025:

'...Does your council currently have a policy governing the use of generative AI by staff? If so, can I please have a copy of the policy? If not, are you in the process of developing such a policy? I'd also welcome any examples of innovative uses of generative AI by your council to support the work it does...'

Please find enclosed Nelson City Council's Policy for use of Artificial Intelligence (AI) at Nelson City Council.

Below are details of two AI initiatives developed to support Council's work.

Analysis of submissions:

With limited time to process community feedback on the Long Term Plan, an innovative approach was needed to efficiently review submissions and deliver insights to elected members. Partnering with a local AI specialist, a tool was developed to streamline the analysis of public submissions by processing over 1,500 entries from a submissions database, undertaking sentiment analysis and identifying key themes. While staff reviewed and verified outputs, the AI tool provided structured, auditable data that informed reporting and supported decision-making. The tool also enabled real-time responses to queries during meetings and was later used to draft personalized replies to submitters, reflecting Council decisions.

As part of the consultation process, submitters were advised that Council was trialling the use of AI tools to help speed up the processing of submissions and reduce the resources used. To ensure the submitter's privacy was protected, only publicly available information was shared with the AI company involved in the project.

This project won the 2024 ALGIM ICT Project of the Year Award.

Enhancing Community Engagement Analysis:

Council's community engagement on infrastructure projects often involves extensive stakeholder conversations. To enhance our engagement with stakeholders, improve productivity and make significant time savings we have developed a solution using two AI tools. Otter.ai is used for automatic transcription of stakeholder conversations which are then provided to an AI company that uses an AI tool (development ongoing) to process the transcripts to generate spatial plans and analytics. This AI solution is currently being used for a major city development and, although in its infancy, there are already many positive outcomes and benefits as a result of implementing this new tool. In line with our protocols, stakeholders are advised of the tools being used prior to conversations commencing.

You have the right to seek an investigation and review by the Ombudsman of this response. Information about how to make a complaint is available at www.ombudsman.parliament.nz or Freephone 0800 802 602.

If you wish to discuss this decision with us, please feel free to contact me.

Yours sincerely

A handwritten signature in blue ink that reads "Nicky McDonald".

Nicky McDonald

Group Manager Strategy and Communications

Encl:

- Policy for use of Artificial Intelligence (AI) at Nelson City Council
- Policy attachment: Privacy Impact Assessment for use with AI Tools

Internal Document ID:

Policy for use of Artificial Intelligence (AI) at Nelson City Council

Contact person for queries: Manager Strategy and Communications

Approved by: Senior Leadership Team

Approval date: 15 April 2024

-
1. Any use of an AI tool integrated into a Council project, activity, or process must be approved by a Group Manager. As an example, this would mean using AI to help analyse submissions for a public consultation would need approval but using AI to improve the text in a report or generating ideas for an agenda would not.
 2. Do not use sensitive, personal or confidential information in an AI tool without Senior Leadership Team approval and, even then, only if you are using a contained system (ie one that is not linked to the internet and where our data is not shared outside Council). NB: Council's Copilot AI tool operates in a contained system.
 3. Even when operating in a contained system, try to remove any sensitive, personal or confidential data first, or if that is not possible then complete a privacy assessment (see form Appendix 1) and have it approved by Council's Privacy Officer (Group Manager Strategy and Communications).
 4. Avoid, if at all possible, inputting into AI tools any information that Council would be likely to withhold under a LGOIMA (Local Government Official Information and Meetings Act) request.
 5. Given the potential for inaccurate or incomplete or out of date outputs, think carefully about using AI tools for projects that are business-critical for Council.
 6. The responsibility for outputs remains with the responsible staff member. AI tools are known to make mistakes and invent material and their input should not be assumed to be correct.

7. A testing regime should be included to verify information from AI where that is key to the performance of a project.
8. Do not use AI tools for work purposes where data may be retained by a third party (usually for the use of further training the AI tool).
9. Consider Te Tiriti o Waitangi and the impact of AI on any Māori data Council may hold or on Council services involving Māori, and work with Māori in such cases.
10. Consider the risk of inbuilt bias in the tool for any projects using AI.
11. Always let the community know when AI is being used and why, in relation to projects involving the public, and let them know how they can access/correct their information.
12. Where staff are working with an external provider using an AI tool in a project for Council:
 - the security of the provider's system needs to be assessed before proceeding;
 - there needs to be clear agreement on what happens to Council's data once any contract ends;
 - responsibilities for incident management need to be clearly defined in the contract.

Appendix 1: Privacy Impact Assessment for use with AI tools

Available [here](#).

Privacy Impact Assessment relating to Artificial Intelligence tools

#	Description of the privacy principle (from the Privacy Act 2020)	Summary of personal information involved and issues for consideration	Assessment of compliance with principle
1	Principle 1 - Purpose of the collection of personal information Principle 10 – Limits on use of personal information Only collect personal information if you really need it. Only use personal information for the purpose it was collected for	Identify each element of personal information that may/ will be collected if you proceed and satisfy yourself that it is necessary for the activity/ project. What is the purpose of collecting the personal information involved here? How will that enable Council to do what it needs to do? Are you only collecting what you actually need? For example, do you really need “date of birth”, or will “age” or “over 18” be enough? How will you ensure the information is only used for the intended purpose?	Comments:
			Note whether compliant or not: ✓ or x
2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible	How is the information to be collected, and who from? If personal information is collected from some source other than the individual, is this appropriate and justifiable?	Comments:
			Note whether compliant or not: ✓ or x

3	Principle 3 – Collection of information from subject Tell them what information you are collecting, where it will be held, who will have access to it and why, what you're going to do with it, whether it's voluntary to provide all or some of the information, and the consequences if they don't provide it.	How will you tell people everything in this checklist? Or will it be so obvious to them that you don't need to spell it out? If you're not going to provide details, which of the exceptions (in Principle 3 of the Privacy Act 2020) applies? NOTE: Many of these aspects may be covered in Council's privacy statements (see Privacy Statements (sharepoint.com) or Council's Privacy Policy (Privacy breach policy and management plan - approved 15 May 2023.docx (sharepoint.com))	Comments: Note whether compliant or not: ☐ or x
4	Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information Take particular care if collecting information from children or young people	This should describe how the information is collected, and should assess whether the method of collection is lawful, fair and appropriate in the circumstances. What is fair and appropriate may look different if you are collecting children or young people's information. Thought should also be given to adjusting collection methods as required for speakers of other languages and those experiencing disabilities where appropriate.	Comments: Note whether compliant or not: ☐ or x

5	Principle 5 – Storage and security of personal information Principle 6 – Access to personal information Principle 7 – Correction of personal information Principle 9 – Do not keep personal information for longer than necessary	How will the information be stored and protected? Consider how you will provide access to the information owner if required Consider how you will correct information if required, including advising any agency that the information has been legitimately shared with about the update Consider how the information will appropriately be disposed of and when? Refer to Council's Privacy Policy (Privacy breach policy and management plan - approved 15 May 2023.docx (sharepoint.com)) and other privacy resources (Privacy Policies and Procedures (sharepoint.com)) for guidance.	Comments: Note whether compliant or not: ✓ or x

6	Principle 8 – Accuracy etc. of personal information to be checked before use Principle 11 – Limits on disclosure of personal information Make sure personal information is correct, relevant and up to date before you use it Do not disclose information unless there is justifiable reason	Think about what steps will be taken to make sure information is correct before use or authorised sharing, and to make sure the Artificial Intelligence tool does not introduce errors. Also consider how damaging would it be if the information is wrong or misleading? The more damaging it will be, the more extensive should the steps be for checking accuracy. If you are going to disclose the information, which of the exceptions (in Principle 11 of the Privacy Act 2020) allows you to do this? Consider how you will ensure unauthorised disclosure does not occur.	Comments:
			Note whether compliant or not: ✓ or x
7	Principle 12 – Limitations on disclosure outside of New Zealand Do not disclose information internationally unless the information will be protected by comparable safe guards to New Zealand	Consider the AI model that is intended to be used (open or closed) and where the servers are located (re storage) – are these in New Zealand? Somewhere with comparable protections (Australia, Europe)? A country without comparable protections (e.g. USA)	Comments:
			Note whether compliant or not: ✓ or x