MINISTRY OF TRANSPORT
TE MANATŪ WAKA

OC250975

13 November 2025

[redacted]

Tēnā koe [redacted]

I refer to your email dated 16 October 2025, requesting the following under the Official Information Act 1982 (the Act):

> *"To better understand the government's use of artificial intelligence (AI), I request the following information:*
> *1. A list of all AI tools that are currently approved for use by staff at your agency.*
> *2. Any documentation outlining the conditions, guidelines, or policies attached to the approval and use of these tools.*
> *3. For each approved tool that is not free to use, please provide the number of paid licenses or subscriptions the agency currently holds. I confirm that I do not require any commercially sensitive information (e.g. licence costs), merely the number of authorised users.*
> *4. Copies of all completed Cloud Risk Assessments and Privacy Impact Assessments (or equivalent documents) for each of the approved AI tools."*

I have answered your questions in turn below.

1. A list of all AI tools that are currently approved for use by staff at your agency.

- CoPilot – publicly available free version
- CoPilot 365 – Enterprise, Paid
- Consensus – AI search engine for research papers, free version
- Claude – currently used only in a pilot phase.

2. Any documentation outlining the conditions, guidelines, or policies attached to the approval and use of these tools.

- Refer to Attachment 1 – Ministry GenAI Guidelines

3. For each approved tool that is not free to use, please provide the number of paid licenses or subscriptions the agency currently holds. - I confirm that I do not require any commercially sensitive information (e.g. licence costs), merely the number of authorised users.

- CoPilot365 – 86 paid users as of 11 November 2025
- Claude – 21 paid users as of 11 November 2025

4. Copies of all completed Cloud Risk Assessments and Privacy Impact Assessments (or equivalent documents) for each of the approved AI tools.

- CoPilot 365 PIA – Refer to Attachment 2

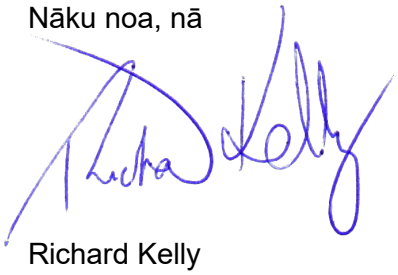
The Ministry AI Guidelines make it clear that any Ministry or government information, or any data that uses personal information must not be used within any AI tools except the Microsoft 365 CoPilot (paid version) with an assigned license. Consequently, the only Privacy Impact Assessment required is the one attached.

All AI products have had security risk assessments completed, but due to the nature of these documents, any security risk assessments have been withheld under section 6(a) of the Act as release would be likely to prejudice the security or defence of New Zealand or the international relations of the New Zealand Government.

You have the right to seek an investigation and review of this response by the Ombudsman, in accordance with section 28(3) of the Act. The relevant details can be found on the Ombudsman's website **www.ombudsman.parliament.nz**

Thank you for writing.

Nāku noa, nā



Richard Kelly
Manager, Business Enablement and Property

MINISTRY OF TRANSPORT
TE MANATŪ WAKA

AI Guidelines

Purpose

The purpose of this guidance is to:

1. Ensure that Ministry staff or contractors who wish to use generative artificial intelligence (GenAI) tools can do so safely[1].
2. Help staff make informed decisions to leverage the opportunities these tools present while actively managing risk.

This guidance outlines how these tools can be used safely, and effectively to generate basic content and to draft or develop ideas This guidance should be read alongside our Digital Services and Privacy policies which apply when using GenAI tools.

What is GenAI?

Generative AI (GenAI) is used widely around the world.

AI	Artificial intelligence refers to the simulation of human intelligence processes by computer systems, including learning, reasoning, problem solving, and decision making.
ML	Machine learning is a subset of artificial intelligence that uses algorithms and statistical models to enable computers to learn from and make predictions or decisions based on data without being explicitly programmed.
Gen AI	GenAI is a branch of artificial intelligence focused on creating computer systems that generate new, original content, such as images, text, music, or other creative outputs. Microsoft Copilot, and ChatGPT, are well-known examples of GenAI.

Potential benefits of GenAI include

- **Efficiency and productivity** through simplification and automation.
- **Improved service design and delivery** through targeting and personalisation.
- **Innovation** from optimisation and access to insight based on larger volumes of data.
- **Improved policy and advice** through faster/better options analysis and explaining complex concepts in plain language.

[1] Refer advice from the Government's Chief Digital Officer (GCDO) around use of GenAI in the public service, February 2025 (https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/responsible-ai-guidance-for-the-public-service-genai)

Key risks of GenAI include

There are risks from the adoption of any new technology. While not exhaustive, key risks from the use of AI include:

- **Confidentiality Risk (policy decisions)**. If seen to be inputting information about confidential policy decisions yet to be made
- **Confidentiality Risk (commercial)**. Inputting confidential or sensitive information into AI tools, such as Ministry data, commercial or supplier's information, risks that information being compromised or disclosed.
- **Privacy Risk.** Risk that personal information is entered into the AI tool and is retained or disclosed by the AI tool or used to continue training it.
- **Security**. Use of unapproved AI tools could allow a bad actor to learn more about the Ministry than we would be prepared to release/share.

Approved applications for use

M365	**Microsoft 365 Copilot**	Paid version accessible through Microsoft suite
	Copilot (Microsoft Edge)	Free version available through Microsoft Edge
Consensus	**Consensus**	AI Search Engine for Research

Use of GenAI tools not listed above to use with Ministry data **must** be reviewed for security risks and approved for use by the Ministry's AI Sponsors – the DCE, Corporate Services and DCE, Sector Strategy. Note there are costs associated with this process.

Process for requesting access to a new tool:

1. Manager to document and submit a brief business case including the benefits you expect from the tool, how the tool differs from those in the existing approved list, along with any licensing costs to the Ministry AI Governance Group (via email to apps@transport.govt.nz – please contact the Business Applications Adviser for more details)
2. Complete a PIA and Risk Assessment with support from the Legal and IT team.
3. AI Governance Group will review the business case and make recommendations to AI Sponsors.
4. AI Sponsors (DCE Corporate Services and DCE Sector Strategy) to approve or decline the request.

When using these tools, you must consider

☑ **Microsoft 365 Copilot (paid version) only –**

You **can** input Ministry or government information, and data that uses personal information[2] into Microsoft 365 Copilot – but **only** if you have been assigned an official Microsoft 365 Copilot license

X **All other AI tools –**

You **must not** input Ministry or government information, or any data that uses personal information into any other AI tools (this includes Copilot for Edge)

X You **must not** use GenAI-created images from **any** tool (including Microsoft 365 Copilot and other AI platforms) in Ministry publications.

☑ You **must** store all final versions of documents in TARDIS

When using these tools, you must

- consider if there is an **appropriate business reason to use the tool**
- **be transparent** about how and where we are using outputs from GenAI tools, including in advice to Ministers or if we plan to use it to review information from external sources (such as public consultation).
- **exercise the same critical thinking and caution that we would use when sourcing information from the internet**
- **check all outputs against verified sources.**
- **treat GenAI as a starting point, not the answer**. GenAI tools are trained on information created by people so they can mirror our biases.
- unless you are using the paid version of Microsoft 365 Copilot[3], assume everything is recorded by the AI tool and "what goes in" stays "in" forever and will be available to anyone, anywhere.
- **carefully consider Te Tiriti** – we must consult and work with Māori where GenAI tools may be being used for Māori data, and its use may impact Māori, including services to Māori use work devices and accounts (rather than personal) to access the approved AI tools when using them for a Ministry purpose.

[2] "Personal information" is any information about an identifiable living person. A person doesn't have to be named in the information to be identifiable.

[3] The paid version of Microsoft 365 Copilot runs in a secure, closed-off environment, and information entered into the system is contained within the Ministry and ***not*** fed back to Microsoft.

How can I safely use AI?

Here are some examples of how you could use Copilot in Microsoft Edge:

a) **summarise publicly available information**
e.g. what are the key messages from a long report),

b) **provide a 'starting point' for work**
e.g. write me a speech about…

c) **ideas generation**
e.g. write me code for this task, tell me about the evidence on what improves productivity in the transport system

d) **work out a calculation**
e.g. how do I calculate the average annual percentage change in deaths and serious injuries in New Zealand?

Review and Approval

Review and Approval: Owner	Approved By	Date Approved	Next Review Date
Manager, Business Enablement and Support	Senior Leadership Team	31 October 2024	October 2025
Chair of AI Governance Committee (Manager, Business Enablement and Property)	Senior Leadership Team	29 September 2025	October 2026

Ministry of Transport
TE MANATŪ WAKA

BRIEF PRIVACY IMPACT ASSESSMENT

CoPilot – M365

11 December 2024

1. Project summary: AI Pilot – CoPilot M365

1.1 Brief description of the project

Based on the successful CoPilot Studios Pilot - 'Setting of Speed Rule 2024' and draft Government Policy Statement on Land Transport 2024' the Ministry of Transport will start to roll out CoPilot licences to end users. With the initial testing phase being 10 licences, utilized in a semi-closed environment for each user.

This pilot leverages Microsoft CoPilot in the Ministry's M365 environment, supporting tasks such as, but not limited to, document analysis, note summarisation and simple documentation tasks. The initiative aims to enhance productivity while adhering to all Ministry privacy policies and the New Zealand Privacy Act.

CoPilot M365 incorporates robust privacy and security measures to protect user data:

- **Data Residency**: Ensures data is processed within designated locations, in this instance only within the Ministry s tenancy.
- **Anonymization**: User prompts and interactions are not stored or used for model training, ensuring personal information is not retained.
- **Enterprise Protection**: Applies controls under the Data Protection Addendum ("DPA")
    - The DPA outlines the data processing and security terms. It specifies the obligations of both Microsoft and its customers regarding the handling of data, ensuring compliance with data protection regulations.
- **Responsible AI Practices**: Adheres to Microsoft's AI Principles and Responsible AI Standard, ensuring ethical data handling.

For further details on Microsoft's Privacy and Copilot Data and Security policies, see:

- Data, Privacy, and Security for Microsoft CoPilot
- Microsoft Privacy Statement

1.2 Personal information that the project will involve

Type of personal Information	Source of Information	Purpose of information for the project
The personal information involved in this pilot is any personally identifying information provided by public.	Provided by public. Though any standard means of contacting the Ministry of Transport.	All information will remain within the Ministry's IT tenancy and will not be used by CoPilot to train its model. This is in line with the Ministry's current privacy policies.

2. Privacy assessment

2.1 Areas that are risky for privacy

Some types of projects are commonly known to create privacy risks. If the project involves one or more of these risk areas, it's likely that a PIA will be valuable.

Use this checklist to identify and record whether your proposal raises certain privacy risks. Delete any that do not apply.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Information management generally			
A substantial change to an existing policy, process or system that involves personal information ***Example**: New legislation or policy that makes it compulsory to collect or disclose information*		✓	
Any practice or activity that is listed on a risk register kept by your organisation ***Example:** Practices or activities listed on your office's privacy risk register or health and safety register*		✓	
Collection			
A new collection of personal information ***Example:** Collecting information about individuals' location*		✓	
A new way of collecting personal information ***Example:** Collecting information online rather than on paper forms*		✓	
Storage, security and retention			
A change in the way personal information is stored or secured ***Example:** Storing information in the cloud*		✓	
A change to how sensitive information is managed ***Example:** Moving health or financial records to a new database*		✓	

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Does the project involve any of the following?	**Yes (tick)**	**No (tick)**	**If yes, explain your response**
Transferring personal information offshore or using a third-party contractor ***Example:*** *Outsourcing the payroll function or storing information in the cloud*		✓	
A decision to keep personal information for longer than you have previously ***Example:*** *Changing IT backups to be kept for 10 years when you previously only stored them for 7*		✓	
Use or disclosure			
A new use or disclosure of personal information that is already held ***Example:*** *Sharing information with other parties in a new way*		✓	
Sharing or matching personal information held by different organisations or currently held in different datasets ***Example:*** *Combining information with other information held on public registers, or sharing information to enable organisations to provide services jointly*		✓	
Individuals' access to their information			
A change in policy that results in people having less access to information that you hold about them ***Example:*** *Archiving documents after 6 months into a facility from which they can't be easily retrieved*		✓	
Identifying individuals			
Establishing a new way of identifying individuals ***Example:*** *A unique identifier, a biometric, or an online identity system*		✓	

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
New intrusions on individuals' property, person or activities			
Introducing a new system for searching individuals' property, persons or premises ***Example:*** *A phone company adopts a new policy of searching data in old phones that are handed in*		✓	
Surveillance, tracking or monitoring of movements, behaviour or communications ***Example:*** *Installing a new CCTV system*		✓	
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information ***Example:*** *Changing the location of the reception desk, where people may discuss personal details*		✓	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them ***Example:*** *Adding a new medical condition to the requirements of a pilot's license*		✓	
List anything else that may impact on privacy such as bodily searches, or intrusions into physical space		✓	

2.2 Privacy assessment

#	Description of the privacy principle (These can be deleted from your final report if they're not relevant to your project – but you should at least consider each principle)	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it	*The pilot will not collect any personal information beyond the status quo.*	*Compliant*	
	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible	*Any information is provided directly by the public. All standard policies will still apply.*	*Compliant*	
	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	*All information provided by the public will adhere to existing internal policies and the Privacy Act. No change to communications on any channel used by the public to submit data.*	*Compliant*	
	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	*The pilot will not collect any personal information beyond the status quo.*	*Compliant*	

#	Description of the privacy principle (These can be deleted from your final report if they're not relevant to your project – but you should at least consider each principle)	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
	Principle 5 – Storage and security of personal information Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	*The pilot does not change the Ministry's existing policy. CoPilot does not store any personal information.*	*Compliant*	
	Principle 6 – Access to personal information People can see their personal information if they want to	*The pilot does not change the Ministry's existing policy.*	*Compliant*	
	Principle 7 – Correction of personal information They can correct it if it's wrong, or have a statement of correction attached	*The pilot does not change the Ministry's existing policy.*	*Compliant*	
	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	*The pilot does not change the Ministry's existing policy or how we handle data.*	*Compliant*	
	Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you're done with it	*The pilot will adhere to all current data deletion and retention policies.*	*Compliant*	

#	Description of the privacy principle (These can be deleted from your final report if they're not relevant to your project – but you should at least consider each principle)	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
	Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies	*The pilot does not change the Ministry's existing policy or how we handle data.*	*Compliant*	
	Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies	*The pilot will not disclose personal information*	*Compliant*	
	Principle 12 – Disclosing information outside New Zealand Only share information with an agency outside New Zealand if the information will be protected	*The pilot will not disclose personal information*	*Compliant*	
	Principle 13 – Unique identifiers Only assign unique identifiers where permitted	*The pilot will not use unique identifiers*	*Compliant*	
	Other privacy interests	*NA*	*NA*	

3. Summary of privacy impact

The privacy impact for this project has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	✓
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	
High – Sensitive personal information is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.	

3.1 Reasons for the privacy impact rating

The privacy impact rating is considered low for the following reasons:

- The use of personal data is minimal and involves standard Ministry processes.
- All data is securely retained within the Ministry's IT systems, following existing data protection protocols.
- The implementation of CoPilot aligns with New Zealand's Privacy Act and the Ministry's privacy policies.
- Section 2 shows there are no privacy risks from the pilot because the information is retained in the same way a standard submissions process is at the Ministry.

4. Recommendation

The Recommendation(s) from the Advisory Group to the Project Sponsor is set out below.

The Governance Group **recommends**:

Note that a privacy assessment has been carried out.

Note that there are no privacy risks from the pilot because the information is retained in the same way the Ministry currently operates.