Whaikaha
Ministry of Disabled People

Scan for
NZSL name

Visual description: A purple Whaikaha logo with a QR scan for the NZSL name.

OIA1172

[redacted]

15 June 2026

Tēnā koe [redacted]

Thank you for your Official Information Act 1982 (OIA) request of 22 May 2026, to the Ministry of Disabled People - Whaikaha (the Ministry), requesting information about use of Artificial Intelligence (AI).

I have answered each of your questions below.

- **What Artificial Intelligence is your Ministry considering implementing in the next year?**

In 2026, the Ministry gave staff the ability to hold a full M365 Copilot licence after completing a Responsible Use of AI for Copilot course (which covers essential AI concepts; strengths, weaknesses and risks of GenAI; using Copilot safely and responsibly; and situations when Copilot should not be used).

The Ministry is looking to implement human controlled AI assistants (also known as "agents" which is Microsoft's technical name) within Copilot that have been designed to:

- support everyday work
- improve consistency and quality
- save time on drafting and admin tasks.

In Appendix 1 you will find a list of the AI assistants being developed and their intended purpose. Once all have been completed and approved, they will be available for staff to use.

Staff holding the licences will also be able to create their own assistants to assist with their work tasks.

The Ministry is also currently evaluating the AI features of a cloud-based stakeholder relationship management platform, in accordance with our AI risk level assessment (more detail about our risk assessment is contained in the response to your final question). This platform is being rolled out to strengthen stakeholder relationship management across the Ministry. Decisions on whether to use its AI functionality have not yet been made.

- **What aspects or parts of the business will it be implemented? Ie how will the AI be used**

Please refer to the answer above and to Appendix 1, which outlines the use of AI in the Ministry. While some of the AI assistants have been designed for specific teams within the Ministry, it is intended that all staff will be able to use these tools to assist with their workloads.

- **Will it's implementation reduce the workload or staff numbers?**

The Ministry is focusing on implementing AI tools that staff use to support their everyday work and save time on administrative tasks.

- **What safety and security protocols has it had to pass to be considered acceptable for implementation?**

The Ministry has a shared services agreement with the Ministry of Social Development (MSD) for IT and Information, Privacy and Security services. Copilot has been through MSD's Certification and Accreditation (C&A) process. C&A is a process that provides MSD with confidence that the delivery of its systems are well-managed and security risks are properly identified and mitigated. MSD also assesses Security, Privacy, Human Rights and Ethics as part of the process, ensuring wider obligations, and obligations under the Privacy Act 2020, are met.

In addition, AI is only used at the Ministry when it is people-centred, risk-assessed, and privacy-safe with human oversight at every step. Only approved AI tools and for approved AI use cases that have gone through the Ministry's risk tiering and approval process can be used by staff.

In Appendix 2 we have attached a copy of the Ministry's AI Business Rules, which guides how AI is used at the Ministry. In Appendix 3 we have attached the Ministry's AI Tool and use case approval process, which maps the steps to be used when the Ministry is looking to implement a new AI tool (or when

looking to use an already approved AI tool in a different way). This is a part of the Ministry's Responsible AI Framework.

If you wish to discuss this response with us, or if you are seeking any further information, please contact OIA_requests@whaikaha.govt.nz.

Please note, as part of its commitment towards increasing transparency, the Ministry intends to make the information contained in this letter, and any attached documents, available to the wider public. The Ministry will do this by publishing this letter on our website. Your personal details will be deleted, and no information that would identify you as the requestor will be released.

If you are not satisfied with this response, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

Emma Williams
Manager, Ministerial and Executive Services

Agent ID	Assistant Name	Risk Level	Approval Status	ELT Endorsed	Intended Audience	Is Personal Use	Business Group	Description
AA01	**Speech Writer Assistant**	2	Approved	Yes	Team	No	Strategy & Enablement	Helps staff co-create first drafts of speeches tailored to the Chief Executive by using provided context and source materials.
AA02	**Meeting Minutes Assistant**	2	Approved	Yes	Team	No	Strategy & Enablement	Helps staff generate structured first drafts of meeting minutes from meeting artefacts.
AA03	**Plain Language Assistant**	2	Approved	Yes	Organisation	No	Strategy & Enablement	Helps staff create clear, accessible content in plain language more efficiently using Whaikaha guidance and knowledge sources.
AA04	**Talking Points Assistant**	2	Approved	Yes	Team	No	Strategy & Enablement	Helps staff draft structured first-pass talking points for events and meetings using relevant source materials and prior examples.
AA05	**Branding & Style Assistant**	1	Approved	Yes	Organisation	No	Strategy & Enablement	Helps staff review and prepare documents to align with Whaikaha templates, branding, style guidance, and accessibility standards.
AA06	**Weekly Report Assistant**	2	Approved	Yes	Team	No	Outreach & Innovation	Helps staff compile inputs from multiple sources and generate draft weekly reports in a standard format for leadership reporting.
AA07	**Events Aide Memoire Assistant**	2	Approved	Yes	Team	No	Outreach & Innovation	Helps staff draft and refine first-pass Chief Executive aide-mémoires for events, meetings, and visits using provided context and standard formats.
AA08	**HR Administrator**	2	Approved	Yes	Team	No	Strategy & Enablement	Helps staff draft employment terms and conditions letters using approved templates, employee data, and HR process guidance.
AA09	**Proofreader Assistant**	1	Approved	Yes	Organisation	No	Policy & Insights	Helps staff check draft documents for spelling, grammar, structure, and style before final human review.
AA10	**Community Feedback Synthesiser Assistant**	2	Development	Yes	Team	No	Policy & Insights	Helps staff be deliering a secondary synthesis and sense-check of community feedback insights, reinforcing and complementing, not replacing human-led analysis.
AA11	**Evidence Scan Assistant**	2	Development	Yes	Team	No	Policy & Insights	Helps staff scope evidence scans, identify and analyse sources, and produce structured draft insights to support evidence-informed work, with human review required.
AA12	**ELT Governance Assistant**	2	Development	Yes	Team	No	Policy & Insights	Support governance processes by preparing and structuring materials for Executive Leadership Team decision-making and oversight
AA13	**Accessibility Tool Assistant**	2	Development	Yes	Team	No	Strategy & Enablement	Helps staff to create acessible, well-structured documents by checking and improving formating
AA14	**Reporting Framework Assistant**	2	Development	Yes	Team	No	Strategy & Enablement	Helps staff compile inputs from multiple project status reports and generate draft reports for different target audience.
AA15	**SRM Prompt Builder Assistant**	1	Development	Yes	Team	No	Outreach & Innovation	Helps project team generate consistent prompts for the Stakeholder Relationship Management (SRM) Change Management Project
AA16	**OIA Search AI Assistant**	1	Development	Yes	Team	No	Outreach & Innovation	Helps OIA staff by searching past OIA files to identify similar requests, reusable material and relevant precedent.

Whaikaha AI Business Rules

These rules guide how we use Artificial Intelligence (AI) at Whaikaha. They are short, practical guardrails for all kaimahi, contractors, and partners. They sit under the Whaikaha Responsible AI Policy and reflect our values, Te Tiriti o Waitangi, Māori data sovereignty, and our commitment to disabled people and tāngata whaikaha Māori.

These rules are mandatory for all internal and external people as defined in the AI Policy. Breaches may be treated as a breach of Whaikaha AI policy and the Public Service Code of Conduct.

See below for a table that links each draft Whaikaha AI Business Rule to the AI Strategy guiding principles and Whaikaha organisational values.

Business Rule header	Business Rules	Linked AI Strategy Guiding Principle(s)	Aligned Whaikaha Value(s)
1. Put people first, and be transparent, accountable and ethical	• AI will never replace human judgement; particularly where people's rights, wellbeing, or access to services are at stake. • Kaimahi must always be in the loop to review, and they remain accountable for AI outputs in their work. This includes a review of AI outputs for accuracy, bias, cultural safety, inclusiveness, and accessibility (plain language, Easy Read, NZSL, alternate formats). For complex, cultural, technical, or high-risk content, a relevant subject matter expert must also review. • Kaimahi will always review AI outputs carefully for hallucinations or potential bias and correct any bias, unfairness, or errors before outputs are used or shared. Ensure regular reviews and sensitivity checks are completed to ensure fair and unbiased AI deployment.	*Our AI use is open, accountable, and we keep our people in the loop.* *Our AI use protects the rights and aspirations of disabled people.* *Our AI use breaks down barriers and supports equitable outcomes.*	Manaakitanga (care, respect, dignity) People-centred (disabled people and tāngata whaikaha Māori at the heart) Integrity Accountability

	• Kaimahi must always be transparent when AI has been used.
	  ○ For external communications (e.g. reports, briefings, social media posts, images, or videos), AI use must be disclosed by noting that content has been generated through an AI-assisted and human-reviewed process. People should use the wording, disclaimers, or visual markers set out in Whaikaha AI guidance and templates. See the Appendix for some templated wording for common applications.
	  ○ For internal use (e.g. drafting, brainstorming, or idea generation), transparency is expected within the relevant team or project, but formal disclosure in the final artefact is not required unless specified. For example, this could be informing your manager that content was AI assisted or generated. this could be informing your manager that content was AI assisted or generated.
	• When recording and transcribing a meeting, kaimahi must obtain consent from participants before recording and transcription begins.
	• Always use AI in ways that respect disabled people's rights and do not discriminate, misinform, or harm kaimahi, disabled people, Māori, whānau, or the wider community.		

2. Use only approved AI tools and use cases	• Kaimahi may only use AI tools for use cases that have been through the Whaikaha AI risk tiering and approval process. • Kaimahi may not enter Whaikaha sensitive information into public or non-approved AI tools. (including Cabinet papers, Ministerial briefings, legal advice, or other classified or confidential information). • Accidental entry of confidential or sensitive data into non-approved AI tools must be reported immediately to your	*We are responsible guardians of data, privacy and sustainability.* *Our AI use is open, accountable, and we*	Integrity and trust Safety Responsibility

	manager. The incident will be managed in accordance with Whaikaha incident response procedures. • If unsure whether an AI tool or use case is permitted, seek advice from your manager or a subject matter expert before use. Refer to linked list of approved AI tools and use cases and subject matter experts in the Appendix of the AI Policy.	*keep our people in the loop.*	
3. Protect privacy, data and culture	• Kaimahi must always comply with the Privacy Act 2020, Official Information Act 1982, contractual obligations, government security requirements such as the NZISM, and Whaikaha security and data privacy policies. This means only using approved AI tools for use cases that meet Whaikaha privacy and security requirements. Unauthorised use of AI tools with sensitive data is a reportable security breach. • Apply data minimisation: only share what data is needed when using or validating AI tools or use cases. • Kaimahi must respect Māori data sovereignty and cultural safety. Where disability-related, health, Māori data, or culturally sensitive information is involved, ensure that AI use with this data is approved, and that the appropriate subject matter experts are consulted for human review to check AI outputs for completeness and accuracy. o Where Māori data is involved, consult the Kaihautū – Chief Māori Advisor, and apply Māori Data Governance Pou (especially on collection, protection, access, quality, and classification). o Treat cultural and disability-related data with care, recognising obligations under Te Tiriti o Waitangi and expectations of cultural safety and trust.	*We are responsible guardians of data, privacy and sustainability.* *Our AI use protects the rights and aspirations of disabled people.*	Honouring Te Tiriti o Waitangi Respect for cultural safety Equity

	• AI tool usage is subject to the Official Information Act 1982 (OIA), just like Teams chats, official text messages, and emails.		
4. Co-design with community	• Involve kaimahi, disabled people and tāngata whaikaha Māori in the design, testing, and approval of AI tools and use cases. Co-design of use cases is required before new AI tools or use cases are implemented - depending on the level of assessed risk tiering, co-design can be commensurate to the level of assessed risk. For example, full co-design might not be required for Tier 1 use cases. Ensure AI initiatives meet the needs of key stakeholders through either consultation or collaboration (depending on the purpose and needs of an AI project) so that tools and practices genuinely meet their needs. . • Ensure AI tools are validated with key stakeholder groups to confirm outputs are accessible, culturally safe, and inclusive. • Use AI only in ways that remove barriers and support equity; never in ways that exclude or disadvantage people or go against Whaikaha values, where applicable.	*Our AI adoption places people at the centre, is built around people's voices and experience, and is shaped through collaboration.* *Our AI use breaks down barriers and supports equitable outcomes.*	Partnership (with tāngata whaikaha Māori and disabled people) Inclusion Equity
5. Commit to continuous improvement	• Complete any required AI training (e.g. foundational and/or required AI tool or use case specific training) before using approved tools. • Follow the Whaikaha Responsible AI framework and processes, the Responsible AI policy, and the Public Service Code of Conduct when using AI. • Share lessons learnt and feedback so we can continuously improve together. • Report any issues, misuse, or breaches (e.g. using non-approved AI tools or use cases, entering confidential or sensitive information, failing to disclose AI use) immediately to your	*We are responsible guardians of data, privacy and sustainability.* *Our AI use is open, accountable, and we keep our people in the loop.*	Continuous improvement Shared learning Responsibility

	manager, alternate party, e.g. DCE, through a formal channel, e.g. AI feedback form, incident request form. • Stay informed of updates to AI guidance and apply them in your mahi.		

Appendix

Application of business rule 1. *Put people first, and be transparent, accountable and ethical*

See below for some templated wording which can be tailored to suit the Whaikaha application of AI business rules. These templates need to be maintained and updated to ensure consistent application in line with the Whaikaha Responsible AI framework.

For this business rule, we suggest the following wording for common scenarios where people are using AI for external communications or internal use:

External or internal use of AI	Scenario	How to apply disclosure	Template wording
External communications	Reports, briefings, Cabinet papers	Add as a foot note or acknowledgement section.	This document contains content generated with the support of approved AI tools and reviewed by Whaikaha kaimahi.
External communications	Social media posts (text, images, videos)	Add a short generic marker or hashtag. For visuals, include a small symbol/marker (e.g. “AI-assisted | Human-reviewed”) in the corner of an image or video tile.	#AIassisted – Content created with AI tools and reviewed by Whaikaha kaimahi.
External communications	Email signatures (if AI regularly supports correspondence)	Add as an optional signature line or disclosure statement.	This correspondence may be supported by AI tools. All content is reviewed and approved by Whaikaha kaimahi.
Internal use	Internal use (drafting,	Add a simple note in the draft header or project document.	Draft prepared with AI support - requires human review.

	brainstorming, Copilot use)		

AI Tool and use case approval process

The AI approval process has been designed to incorporate existing technology processes (e.g. currently delivered by MSD) and to integrate specific AI risk approval steps aligning with defined risk appetite, risk level assessment, and newly developed AI policies, practices and business rules. This templated process map can be used when Whaikaha are looking to implement a new AI tool or when you are looking to use an already approved AI tool in a fundamentally different way (e.g a new use case).

1. Identify Risk Level

- Determine the Risk Level of the AI tool or use case using the AI Risk Level Assessment template.
- Work with the DCE Strategy and Enablement (and/or relevant AI risk lead / delegate for the respective organisational area) to ensure the Risk Level is appropriate based on the initial information.
- Confirm that use of the AI tool complies with relevant technology acceptable use policies (e.g. approved applications only, no sensitive data entered into unapproved AI tools).
- Consider whether data protection, data privacy, and security requirements, are met.
- Identify any initial additional mitigations, controls, or other guardrails.

2. Risk Level Approval

- **AI Risk Level 1 (minor risk):** Approval by business/system owner (Tier 3/4 staff).
- **AI Risk Level 2 (moderate risk):** Approval by DCE Strategy and Enablement and one other ELT member.
- **AI Risk Level 3 and 4 (Major or Severe risk):** Requires full ELT approval, including the CE and all DCEs. SMEs should be consulted and collaborate with relevant team members as part of the risk assessment process.
- Approvals must confirm:
  - A bias and cultural safety review has been completed;
  - A named staff member is in the loop to review AI outputs before they are used externally, ensuring accountability for quality, accessibility, and cultural safety;
  - Community co-design and/or participation has been conducted where the AI tool or use case is used by, or has a direct impact on, the community.
- Cover off any conditions set in approval through the next stage.

3. Technology Approval Processes

- Align with existing technology approval processes (e.g. architecture review, change management (e.g. CAB)).
- Address conditions identified during risk level assessment before approval can proceed.
- Approvals must demonstrate:
  - data handling complies with existing standards;
  - no unapproved software or tools are used;
  - planned training, testing, and feedback steps have been considered with appropriate activities in place or planned to be completed as part of Step 5.
- Approvals presented through relevant governance forums if above a certain risk level assessed, e.g. risk level 2-4.

4. Governance sign-off (if required)

- Full ELT, including the CE and the DCEs, provide final approval for higher-risk AI tools or use cases (assessed as AI Risk Level 3-4).
- Note that for level 3 and 4, Māori advisor, comms, and technical SMEs may join governance forums for risk assessment and co-design input.
- RAC does not approve individual cases but receives risk reporting to inform oversight and assurance. This reporting should also show how all Responsible AI and associated risk processes have been made operational.
- A technical change management plan may be required to explain how identified risks are addressed and how the change will be deployed into production (introduced into a "live" environment). *Note this is separate from any required business change activities (see step 5).*

5. Go-live and Monitoring

- Carry out business change management, training, and access protocols in line with existing policies and processes.
- Engage on an ongoing basis with teams on business needs and experience with the AI tool or use case.
- Monitor the AI tool to confirm functionality is maintained and use case application and key risks remain within appetite.
- Encourage a "speak up" culture where staff can raise issues about AI output quality, bias, or other risks.
- Log identified AI risks centrally so this can be tracked with risk mitigations or risk acceptances in place. Ensure risks are escalated to the relevant stakeholder groups depending on level of risk identified.
- Log and escalate any AI-related incidents through existing Service Desk processes (and incident management system), in line with Whaikaha internal risk management or escalation processes.

6. Governance Update and Review

- Report to ELT and RAC every 6-12 months on AI use, new or emerging risks for consideration, risk exposure, and policy and operational effectiveness.
- Consult the DCE Strategy and Enablement (and/or relevant AI risk lead / delegate for the respective organisational area) for approval of enhancements or changes to the AI tool or use cases.
- Ensure reviews cover cultural safety, Te Tiriti o Waitangi, Māori data sovereignty, and accessibility, and alignment with the Responsible AI framework.
- Incorporate feedback from staff, disabled people, tāngata whaikaha Māori, and partners.
- Escalate significant risks or breaches in line with defined risk management framework and processes.

Ongoing Monitoring and AI Governance Oversight

- Regularly review the effectiveness of controls and compliance.
- Consider opportunities for streamlined approvals (e.g. Risk Level 1 use cases, bulk approvals for repeated low-risk use), provided these are pre-agreed with governance forums and remain within risk appetite.
- Maintain risk appetite to reflect changing AI maturity over time.
- Update and oversee AI-related policy and frameworks in line with existing IT standards.
- Escalate or re-level AI risks when needed.
- Provide independent assurance through RAC and regular governance reporting.