



30 July 2026

Tēnā koe

Official Information Act request

Thank you for your email, which was forwarded to our department on 04 June 2026, requesting information about AI guidelines for Jobseeker Support (JS) applications. You requested:

- *Are you able to please share with me the AI guidelines that are being using for the Job Seeker selection process? I was not aware that AI was being used and want to understand where my sensitive data is going and the governance and guardrails being used to protect PII data. Is my personal data being shared with the overseas large language models (LLMs) like Microsoft?*

I have interpreted your request as relating to how the Ministry of Social Development (the Ministry) uses artificial intelligence (AI) to support job seekers and have considered your request under the Official Information Act 1982 (the Act). Please find my decision on your request is set out below.

Personal information is not being shared with overseas Large Language Models (LLMs) in a way that would expose or transfer Personal Identifiable Information (PII) outside of the agreed governance and security controls.

Ministry staff have access to one generative AI tool, Microsoft Copilot Chat, which is used as a general productivity tool. It is not used to analyse client information or provide advice or decisions about clients.

The Ministry also uses a non-generative AI voice recognition tool, available to clients on an opt-in basis. This tool enables Ministry systems to securely verify a client's identity when they contact the Ministry, reducing the need for them to answer multiple security questions when speaking with contact centre staff.

In addition, the Ministry also uses an algorithm within its digital employment platform to help match job seekers with suitable employment opportunities. This tool is not generative AI and is designed to support connections between job seekers and employers. It does not make decisions on behalf of the Ministry.

Any use of AI within the Ministry must comply with the Ministry's AI Policy and undergo assessment through the Certification and Accreditation (C&A) process. Where relevant, this would include assessment through our Privacy, Human Rights and Ethics framework and our Model Development Lifecycle, as described on the

Ministry's website, here: www.msd.govt.nz/about-msd-and-our-work/work-programmes/initiatives/phrae/index.html.

The Ministry also makes use of some other non-generative AI tools that support our client service functions but are not used in interactions with jobseekers. These include:

- Audio transcription to help categorise inbound calls (not used to inform decisions about individual clients)
- Predictive models to support forecasting of demand for services.

I have attached the following document which outlines the Ministry's policy for AI tools approved for use by Ministry staff:

- **Appendix One** - The Ministry's Artificial Intelligence Policy.

I will be publishing this decision letter, with your personal details deleted, on the Ministry's website in due course.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with my decision on your request, 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

pp. 

Anna Graham
General Manager
Ministerial and Executive Services

Artificial Intelligence Policy

Last Review Date:	March 2026
Next Review Date:	March 2027
Approved by:	Leadership Team March 2026
Owner:	GM Information, Privacy, and Security (CISO, CPO); GGM Improvement, Systems, and Technology

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) to use Artificial Intelligence (AI) in ways that best support its aims while upholding its responsibilities to the New Zealand Government and public.

The principles found in this policy set the governing direction and intent for the Ministry's use of AI. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's Information culture and decision-making.

Policy Statement

The Ministry holds and uses information about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

Considered and effective use of AI has the potential to strengthen public services and deliver better outcomes for all New Zealanders. However, if used without proper consideration and appropriate controls, AI can cause harm quickly and at wide scale to both Government and public. The Ministry has a responsibility to manage these risks, and to use AI systems in ways that are human-centric and that create value for New Zealanders.

Scope

This policy applies to all AI systems (see definitions).

This policy applies to all Ministry staff including contractors; and all activity conducted by third parties on behalf of the Ministry.

Policy principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry invests in AI strategically and uses it in line with its values and commitments

The Ministry invests in AI (and its ongoing maintenance and assurance) where there is a clearly identified business need that is most effectively met through this technology. AI systems are used where they can best support our strategic goals, and only where they can be shown to align with our commitments under the Public Service AI Framework, Data Protection and Use Policy, and Algorithm Charter¹. Investment into AI systems is paired with investment into Ministry staff, so that its value is best realised and our staff are best positioned to use it safely.

2. AI systems, and any information assets they consume or produce, are fit-for-purpose to improve outcomes

AI systems are appropriate for their intended use and have the necessary accuracy and reliability required to consistently produce expected results. These systems are used only where the information they rely on is of sufficient quality to meet those requirements. Accuracy and reliability requirements are set and assessed against each individual use case, and only used where these requirements are met.

3. AI systems must be managed in line with their risk profile and potential for harm

AI systems are assessed for potential material impact and only deployed if they have been approved by the Ministry's AI Assurance Officer after due consideration of their potential benefits, risk, and alignment with our values (and where relevant, informed by consultation with key stakeholders). Once approved, they are regularly monitored to ensure that these risks remain managed and that quality is maintained, and if issues are identified corrective action is taken. Assurance of AI systems is ongoing and risk-based, and builds on the Ministry's other assurance frameworks, including certification and accreditation.

¹ [Public Service AI Framework](#); [Data Protection and Use Policy \(DPUP\)](#); [Algorithm Charter for Aotearoa New Zealand](#)

4. The Ministry is transparent with its use of AI systems and AI generated information

Transparency on the use of AI is important for maintaining public trust. The Ministry publishes information about any AI systems it has assessed as having potential material impact, including who is responsible for them and how they are used and why. The Ministry also publishes general information about how we use AI even when there is no potential impact.

AI generated information can vary in reliability and needs to be used with caution. Where information is created primarily or solely by AI systems, that information is marked as such. If that information is used (including to inform decision-making), any resulting information is also marked to show how AI was involved. Being clear about how and when AI information is used is a key component of using AI systems responsibly.

5. Responsible use of AI systems is everyone's responsibility

Ministry staff are responsible for their own use of AI systems, use approved systems, and only use them in ways that align with our values and which keep people and their information safe. Information sourced from AI systems is always used with care and only relied on where it has been verified. Ministry governance and processes play a key role in providing a layer of protection over the potential harms from AI systems, and our awareness of information risk and its acceptable use is just as important.

Responsibilities

Person/Party	Responsibilities
All Staff	All staff are responsible for: • Complying with the Ministry's information and technology policies and standards; • Following any guidance, processes, or procedures for the use of AI systems; • Completing any required training before using AI systems; and • Using AI responsibly in line with this policy.

Person/Party	Responsibilities
Managers	All managers are responsible for: • Ensuring their teams are familiar with the Ministry's requirements under this and other policies; • Understanding and communicating with their teams Ministry expectations around the use of AI systems; and • Modelling good information practice through their actions and behaviour.
Leadership Team	The Ministry's leadership team is responsible for: • Setting strategic direction for our investment in, and use of, AI systems in support of the Ministry's overarching strategic objectives; and • Championing the responsible use of AI systems.
Information Governance Committees	Information Governance Committees are responsible for Overseeing and tracking the achievement of the Ministry's strategic objectives, including how those objectives are being met through our use of AI systems. These governing bodies also have oversight of: • Information and technology guardrails for AI systems; and • Ministry decisions about ensuring there are adequate systems, processes, and controls in place to identify and manage information risk. These committees are further described in the Ministry's Information Governance Policy.

Person/Party	Responsibilities
AI Assurance Officer (AIAO)	The Ministry's AI Assurance Officer is accountable for assuring the Ministry's use of AI systems and is responsible for: • Assessing and where appropriate approving the use of AI systems, contingent on those systems also meeting all other Ministry requirements (including certification and accreditation); • Seeking external expertise where required to support this assessment; • Providing direction on the development of suitable guardrails to manage AI risk; • Setting requirements for the monitoring of AI systems and ensuring that appropriate reporting is carried out; • Overseeing the ongoing assurance of AI systems; and • Communicating externally on the Ministry's use of AI systems through directing the publication of information about these systems, reporting to DIA on AI use, and engaging with counterparts in other agencies on shared initiatives. At the Ministry, the AI Assurance Officer is the DCE Organisational Assurance and Communication. The requirements of this role are derived from the GCDO's AI Assurance Framework.
Emerging Technologies Advisory Group (ETAG)	The Ministry's Emerging Technologies Advisory Group is responsible for: • Providing advice to the AI Assurance Officer and to Information Governance Committees on the potential use of AI systems; • Enabling the Ministry to safely innovate with AI through providing guidance on proposals to key stakeholders; and • Supporting the development of suitable guardrails for AI systems.
System Owners of AI systems	Each AI system must have an identified System Owner, who is responsible for: • Ensuring that the AI system is monitored and that where issues are detected that these are addressed; • Ensuring that any technical controls required for that AI system remain in place and effective; and • Ensuring that the AI system remains compliant with all applicable Ministry policies and standards, including certification and accreditation.

Person/Party	Responsibilities
Information Asset Owners	Information Asset Owners are responsible for: • Understanding how and why the Information Assets they are accountable for used or produced by AI systems; and • Ensuring that any risks to those Information Assets through those AI systems are appropriately monitored and controlled.
Improvement, Systems, and Technology (IST)	Improvement, Systems, and Technology are responsible for: • Investing in and maintaining AI systems in line with Ministry strategy and policy; • Developing and maintaining guardrails for the integration of AI systems into the Ministry's technology environment; • Supporting System Owners to carry out their responsibilities; and • Working with other business groups to identify where business needs could potentially be met through use of AI systems.
Information, Privacy, and Security (IPS)	Information, Privacy, and Security are responsible for: • Leading assurance over the Ministry's use of AI systems through our information assurance framework and activities; and • Developing and maintaining guardrails for the responsible use of information with AI systems, including as this pertains to privacy, human rights, and ethics.
Strategy and Insights (S&I)	Strategy and Insights are responsible for: • Developing and maintaining guardrails for the development, refinement, and maintenance of AI models; • Developing and maintaining guardrails for the use of AI systems in analytics and reporting; and • Developing and maintaining guardrails for data used or produced by AI systems, including code developed to transform or assess that data.

Definitions

Word/ phrase	Definition
AI system	AI systems are defined as in the Public Sector AI Framework. An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Some examples of AI systems are Generative AI systems (such as ChatGPT), predictive models, and computer vision systems.
Algorithm	A procedure or formula for solving a problem or carrying out a task. All AI systems involve algorithms, and as such, requirements in Ministry policies that apply to algorithms also apply to AI systems.
Guardrails	Guardrails are the rules and guidance that keep us safe and delivering value in a direction consistent with organisational strategies and aspirations. A Guardrail could be any documented, approved, and re-usable material which is referenced to understand "what good looks like." Some examples of guardrails are policies, standards, guidance, processes, blueprints, and patterns.
Material impact	Material impact is as defined in the Algorithm Charter. An AI system has potential material impact if it could reasonably be expected to affect the rights, opportunities, or access to critical resources or services of individuals, communities, or other groups in a real and potentially negative or harmful way, or that could similarly influence a decision-making process with public effect.

Related policies

Policy or guardrail	Description
Information Governance policy	Policy requirements for how the Ministry governs information, including where it is used with AI systems.

Policy or guardrail	Description
Privacy, Human Rights, and Ethics policy	Policy requirements for how the Ministry uses information responsibly, including where it is used with AI systems. Includes specific requirements for the use of algorithms.
Information Security policy	Policy requirements for how the Ministry maintains the security of information, including where it is used with AI systems.
Acceptable Use of Technology policy	General policy requirements for staff use of Ministry systems.
Automated Decision-making Standard	Additional requirements for the use of automation (including through AI) in decision-making in some circumstances.
Certification and Accreditation Standard	Requirements for the certification and accreditation of systems.