14 November 2025

s 9(2)(a)

Official information request
Our ref: R001321

Tēnā koe s 9(2)(a)

Thank you for your Official Information Act 1982 (OIA) request received by the Ministry for Regulation (Ministry) on 17 October 2025. You requested:

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.*

Request partially granted
I have decided to partially grant your request. The AI tools approved for use by Ministry staff are:

- Microsoft 365 Copilot
- ChatGPT
- Anthropic
- Gemini
- Napkin AI

The Ministry's AI policy, enclosed as **Appendix A**, sets out how AI may be used within the Ministry.

Additionally, the Ministry refers to the all-of-Government guidelines on the use of technological tools (including AI):

- Responsible AI Guidance for the Public Service (digital.govt.nz)
- The Artificial Intelligence Guidance (data.govt.nz)
- Artificial intelligence and the Information Privacy Principles
- 2024 cross-agency survey of use cases for artificial intelligence (digital.govt.nz)
- Public Service AI framework (digital.govt.nz)

The Ministry holds 109 paid Microsoft 365 Copilot licences.

Information withheld

We are withholding the assessments related to the tools listed above because they contain sensitive information about security measures and possible weaknesses. Sharing this information could make the Ministry's systems vulnerable to attack. For this reason, the information is withheld under section 9(2)(k) of the Official Information Act, to prevent the disclosure or use of official information for improper gain or improper advantage. As required by section 9(1) of the OIA, I have considered whether the grounds for withholding the information requested is outweighed by the public interest. In this instance, I do not consider that to be the case.

Right of review

If you wish to discuss this decision with us, please contact hello@regulation.govt.nz.

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

Please note that we may publish this response (with your details removed) on the Ministry for Regulation website.

Ngā mihi

s 9(2)(a)

Aisling Risdon
Head of Ministerial Services
Ministry for Regulation

Internal policy | Artificial Intelligence

Version	1.0	**Contact**	Digital and Insights Team
Policy Owner	DCE, Organisational Enablement	**Approved**	29th April 2025
SharePoint	Internal policies	**Due for Revision**	April 2026

Context

The Ministry for Regulation (MfR) acknowledges the transformative potential of Artificial Intelligence (AI) in enhancing our operations, boosting efficiency, fostering innovation, and elevating the quality of advice we provide.

We are enthusiastic about embracing these technologies to unlock new opportunities and drive positive change. At the same time, we recognise the inherent risks associated with AI.

This policy is designed to empower MfR staff to responsibly adopt and maximise the benefits of AI, while ensuring its use aligns with principles of safety, transparency, and ethics, and upholds the Ministry's Social License to Operate.

Scope

This policy applies to all MfR **staff** (permanent employees, fixed term employees, secondees, consultants and contractors) at the Ministry for Regulation (**the Ministry** or **we/our**) when using artificial intelligence (AI) to create or process information for the Ministry.

AI is a broad discipline with multiple branches, all focused on creating machines capable of augmenting human intelligence. AI includes Machine Learning (ML), Generative AI (GenAI), Large Language Models (LLM) and Generative Pretrained Transformers (GPT).

The primary focus of ML is to enable machines to learn from past data, improve their performance, and make decisions without explicit coding. Google's search algorithm is an example of ML in its use of past data to refine search results. ML also represents an example of 'narrow AI' which focuses on specific tasks.

GenAI and its subsequent forms, LLM and GPT can process inputs to generate and construct new data. These fall under the category of **'General AI Systems'** which can understand, learn and apply knowledge in multiple domains and can solve problems using machine equivalents of human reasoning, 'common sense', abstract/contextual understanding.

This policy therefore applies to the use and application of all 'General AI Systems' such as Copilot, ChatGPT, Open AI, Gemini, DALL E and Claude, herein referred to as an AI system.

This policy is also to be considered in conjunction with:

- the requirements of the information and records policy Internal policy | Information and Records Management Policy
- the requirement for acceptable use by staff of Ministry information systems in the acceptable use policy Internal policy | Acceptable Use Policy;
- the information security requirements in the protective security policy Internal policy | Protective Security;
- privacy protection in the privacy policy Internal policy | Privacy.

Principles

Background

With the recent increase in the availability and potential of AI to transform how our business can interact, engage and operate, the Ministry has opportunities to boost productivity, augment staff capabilities, improve the quality of Ministry advice, and to more efficiently and effectively deliver Ministry goals.

As AI systems continue to evolve, developing greater predictive capabilities, there is a need to ensure that AI is utilised in a safe, transparent, ethical, and just way that reflects the Ministry's Social License to Operate (SLO).

There are however risks associated with AI usage which need to be managed to support and empower Ministry for Regulation ('the Ministry') staff to innovate, safely adopt, and derive benefits from using AI systems, including:

- Ensuring Ministry staff act in responsible ways that align with the Ministry's existing policies by setting clear expectations for the use of AI systems,
- Continuing to safeguard the confidentiality, integrity and availability of its information,
- Maintaining the privacy of personal information it holds,
- Ensuring the Ministry retains ownership of and responsibility for its advice,
- Ensuring usage is aligned to the government's Māori Data Governance model:
  Co-designing Māori data governance - data.govt.nz and
- Ensuring AI results and recommendations are subject to oversight by accountable staff with appropriate authority and capability at every stage.

As per the NZ Information Security Manual (NZISM), the Ministry's Chief Information Security Officer (CISO) is responsible for setting the strategic direction for information security within the Ministry. While some public sector agencies have opted to ban the use of AI systems, the Ministry in consultation with our CISO, has endorsed the use of authorised AI systems on Ministry devices. This is so we don't create stigma or fear in a technology area that is continually evolving.

Principles

The public service System Lead for AI is the Government Chief Digital Officer (GCDO). The Office of the GCDO provides a Public Service AI Framework and guidance for the public service at this link: Public Service AI Framework | NZ Digital government

The OECD's values-based AI principles inform the principles of the Public Service AI Framework:

Inclusive, sustainable development

Public Service AI systems should contribute to inclusive growth and sustainable development through a focus on innovation, efficiency and resilience, and on reducing economic, social, gender and other inequalities and protecting natural environments. AI use should consider and address concerns about unequal access to technology.

Human-centred values

Public Service AI use should respect the rule of law, democratic values and human rights and labour rights through the lifecycle of each AI system or product. These rights and laws include personal data protection and privacy, dignity, non discrimination and equality, self-determination and autonomy. Public service workers have the right to be consulted on changes made to their work and working arrangements. Agencies need to provide human oversight throughout the AI lifecycle to ensure ethical and appropriate use.

Transparency and explainability

The Public Service needs to commit to transparency in its use of AI. People interacting with government AI systems or receiving AI-assisted services should be aware of and understand how AI is being used. To support this, agencies should publicly disclose when AI systems are used, how they were developed and how they affect outcomes — as relevant and appropriate according to the given use case. Agencies should also enable people affected by the outcome of an AI system to understand how the outcome was determined.

Safety and security

Public Service AI systems should treat the security of customers and staff as a core business requirement, not just a technical feature (security by design). They should minimise risk to individual or national safety and security under normal use, misuse or adverse conditions. The Public Service should ensure traceability of data, apply a robust risk management approach and work collaboratively with commercial and security colleagues in the procurement and assurance of AI tools.

Accountability

AI use within the Public Service should be subject to oversight by accountable humans with appropriate authority and capability at every stage. This should include the application of relevant regulatory and governance frameworks, reporting, auditing and/or independent reviews.

Agency AI capabilities need to keep pace with technological changes, to maintain a strong understanding of AI systems and their limitations.

The Ministry commits to regularly reviewing, refreshing, and re publishing these guidelines to reflect updated guidance from the Office of the GCDO, updated Ministry policy advice, developments in technology, opportunities and risks.

Implementing this policy

The following expectations are aligned to the Ministry's Internal policy | Information and Records Management Policy, Internal policy | Protective Security, Internal policy | Privacy and Internal policy | Acceptable Use Policy policies.

Provided Ministry staff comply with these guidelines, the risks are acceptable when compared to the benefits that are likely to be gained from responsible use of AI systems.

1. **Use of Ministry devices:** For work purposes, a Ministry-managed device must be used to access only AI systems on the Ministry's Allowlist. Note that the Ministry already blocks access via its IT security firewall to some AI systems (eg DeepSeek) until the completion of a satisfactory cyber security, information and privacy risk assessment.

2. **Classified information:** Official Ministry information, classified, personal or other information that would not normally be publicly available must not be 'fed into', submitted, or provided to, any AI system except for Microsoft Copilot because it operates within the Ministry's protected M365 tenancy. Staff must apply the same security best practices used for all Ministry information and data.

3. **Registration**: The Ministry's staff email address must be used when using AI systems for Ministry business purposes. This enables the Ministry to understand system performance, usage, associated costs and respond to requests for information on Ministry AI usage or any investigative needs.

4. **Protect Māori data sovereignty**: The Ministry has an expectation to act in accordance with Te Tiriti o Waitangi principles. The input and/or production

of data and information pertaining to Māori people, language, culture, resources or environments must be done in accordance with the government's Māori Data Governance model and consultation with, or under the advisement of, established Te Tiriti partners to understand and actively manage the impacts of AI for Māori. Ministry staff should be aware that current AI systems may have omissions in authentically representing indigenous cultures. Ministry staff must consult with the Digital and Insights team on appropriate protocols.

5. **Information breach:** Any information breach (or concern that such has occurred) must be reported immediately, in accordance with the Ministry's Internal policy | Protective Security

6. **Decision making:** An AI system must not be empowered to make a business decision.

7. **Use good judgement and validate outputs:** Ministry staff must judge whether the use of an AI system is appropriate, and appropriately scrutinise, validate, and verify any output from an AI system to be used by the Ministry.

8. **Disclosure**: If an AI system has been used to produce a document, then the contribution from the AI system must be disclosed within the document as an integral part of that document's provenance. Identify AI generated text in a footnote in formal documents.

9. **Compliance with security policies:** When using AI systems**,** Ministry staff must use the same security practices used for all Ministry information. This includes using strong passwords, keeping software up to date, and following the Ministry's Internal policy | Protective Security, Internal policy | Information and Records Management Policy and Internal policy | Privacy policies.

10. **Ethical considerations:** In addition to the statements above, use of AI systems must align with the Algorithm charter for Aotearoa New Zealand Charter and be transparent. Ethics and human rights must be considered.

11. **Ministry staff must understand the risks of using AI systems:**
    - AI systems can get things wrong and 'hallucinate' incorrect facts

- AI systems can be biased and gullible when responding to leading questions
- The Ministry has an obligation to consider Māori perspectives in our work; AI system bias can raise questions regarding Māori and indigenous information sovereignty, which can breach Māori tikanga by undermining Māori rangatiratanga
- AI systems can be coaxed into creating toxic content and can be prone to 'injection attacks'
- AI systems can store all the information submitted to it, including the identity of requestor; and once information is submitted to the AI system, the Ministry can expect to have no control of the information or how it is used
- AI systems are rapidly evolving, risks can be underexplored, and new developments can bring new risks
- Public attitudes – including social licence – towards AI in general is very unclear
- An AI system is only as good as the information upon which it is trained.

12. **Assume human intervention**: Ministry staff must always assume that another human has access to interactions with AI systems. Ministry staff must be mindful of the information provided and how it might be used maliciously to reflect poorly on yourself, others, or the Ministry. Ministry staff must ensure interactions only contain information that is already publicly discoverable.

13. **Do not use GenAI for legal advice or guidance:** AI systems must not be used to provide legal advice. However, AI systems may be used to help summarise legislation, notes or legal research and commentary.

14. **Automation:** Only Ministry Allowlist AI systems must be used to assist with automation such as handling repetitive tasks, processing or profiling information for contact or customer relationship management, scheduling appointments or processing information. These activities must be managed by Ministry Allowlist AI systems where there are sufficient agreements and information protections in place e.g. Copilot and automation tools such as Power BI and Power Automate available within the Ministry's M365 platform.

15. **New AI systems:** The Ministry is open to critically evaluating any request by Ministry staff who are interested in using a specific AI system for their

Ministry activities. Any such request must be made to the Head of Digital and Insights. Following a cyber, information and privacy risk assessment, the AI system will be considered for inclusion on the Allowlist.

Ministry staff can do this…

Copilot is the preferred AI tool for Ministry use. The Ministry has invested and will continue to invest heavily in Microsoft 365 (M365) as its strategic productivity and collaboration platform. Ministry staff can use Copilot to analyse and summarise Ministry information including submissions data because, by operating on data only in the Ministry's M365 tenancy, this means that the safety, security and control of data remains with the Ministry.

Ministry staff can also access ChatGPT, Gemini, Perplexity and other AI systems on our "Allow List" via your browser.

Ministry staff can ask ChatGPT, Gemini, Perplexity and other AI systems on our "Allow List" questions on information already in the public domain.

- eg can you provide me with a Risk Management framework to assess environmental risks?
- eg can you provide a summary, from the New Zealand Ministry for Regulation Strategic Intent 2024/25-2028/29 document published on its website, of its role in regulatory system leadership?
- eg can you give me a template for a Project Brief for initiation?
- eg who are the regulatory agencies in New Zealand?
- eg what is the purpose and objectives of the New Zealand Financial Markets Authority (FMA)?
- eg can you provide a comparison between hairdressing regulations in Sweden and New Zealand?

Except for Copilot, Ministry staff can't do this…

Upload any data in any form to other AI systems eg ChatGPT, Gemini, Perplexity

This means, no we can't ask other AI systems to summarise Ministry information that is not already in the public domain.

So, this means, for example, we can't upload submissions data to other AI systems eg ChatGPT, Gemini, Perplexity.

Related policies and more information

1. Public Service AI Framework | NZ Digital government
2. Co-designing Māori data governance - data.govt.nz
3. Algorithm charter for Aotearoa New Zealand - data.govt.nz
4. Internal policy | Information and Records Management Policy
5. Internal policy | Protective Security
6. Internal policy | Privacy
7. Internal policy | Acceptable Use Policy

Glossary

The following terms are used in this policy:

- **Allowlist**: An allowlist, also known as a whitelist, is a security measure that specifies a list of trusted entities (like IP addresses, websites, applications, or email addresses) that are granted permission to access a system or network, while all others are denied access by default. For the Ministry this means automatically blocking all AI systems by default and then only permitting those we wish to allow.

- **Artificial Intelligence (AI)**: The field of software engineering that creates services that, without explicit programming, can generate outputs for particular sets of inputs.

- **Generative AI (GenAI)**: A system that once prompted or questioned generates text or images or other content that closely resembles human-created content. GenAI works by matching user prompts to patterns selectively downloaded from the Web within a Large Language Model (LLM), then using 'neural networks' to probabilistically 'fill in the blank', along the

lines of predictive text messaging. ChatGPT is an example of a GenAI service. Many other GenAI services are available or are under development.

- **Hallucination**: A response by an AI system that may be false or distorted because of the characteristics of the content within the LLM, or the neural network used within the AI system.

- **Injection attack**: A cyberattack where an attacker supplies untrusted input to an AI system which alters the underlying LLM or the course of the system's execution, and allows attackers to access, steal, or compromise the system's information, the system itself, or users' information.

- **IT Security Firewall**: A network security device that monitors and filters incoming and outgoing network traffic based on an organisation's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet to protect a network or system from unauthorized access.

- **Māori Data Sovereignty**: Refers to the inherent rights and interests of Māori in relation to the collection, ownership and application of Māori data.

- **M365 Tenancy**: A private dedicated, isolated instance of M365 services, like Office 365, Azure, Intune, etc., assigned to a specific organisation, where all data and user accounts are stored securely.

Appendix 1 – Approved AI systems

The Ministry is enthusiastic to empower Ministry staff to innovate, safely adopt and derive benefits from using AI systems. An appropriate cyber, information and privacy risk assessment has been satisfactorily completed on Ministry approved AI systems.

Product	Description	Approval date	Approved by *
THE MINISTRY'S PREFERRED AI TOOL is COPILOT which operates within the Ministry's M365 secure platform			
Microsoft Copilot Studio	Microsoft Copilot Studio is a powerful, cloud based platform that allows organisations to build, customise, and deploy AI powered copilots and autonomous agents tailored to their business needs. It's part of the Microsoft Power Platform and integrates deeply with Microsoft 365, Dynamics 365, and other enterprise systems.	23/05/2025	CISO/HoDI
Microsoft Designer	Microsoft Designer is a web-based graphic design tool powered by Copilot AI, designed to help users quickly create professional quality visuals for social media, presentations, marketing materials, and more—without needing advanced design skills.	23/05/2025	CISO/HoDI
Microsoft 365 Copilot Chat	Copilot Chat is a conversational AI feature within Microsoft 365 that allows users to interact with their work data using natural language. It's part of the broader Microsoft Copilot experience and is designed to help users be more productive by making it easy to ask questions, get summaries, and automate tasks—all through a chat interface. It can access and reason over your emails, documents, meetings, and chats (with appropriate permissions) to provide relevant, personalised responses. Ask things like "What were the key points from last week's meeting?" or "Summarize the latest project update email." Summarise long email threads or documents. Draft emails, reports, or presentations based on your prompts. Analyse Excel spreadsheets and generate insights or visualisations. Create formulas or pivot tables based on natural language queries.	23/05/2025	CISO/HoDI

	Schedule meetings, set reminders, or manage tasks in Outlook and Teams. Help prepare for meetings by summarising past conversations and documents. You can chat with Copilot in a Teams-like interface to ask questions or give instructions. It understands context from your Microsoft 365 environment, making it more personalised and relevant.		
Microsoft 365 Copilot (Paid version)	Microsoft 365 Copilot—is a premium AI assistant designed to enhance productivity, creativity, and decision making across an organisation. It integrates deeply with Microsoft 365 apps like Word, Excel, Outlook, Teams, and PowerPoint, and is tailored for enterprise environments with robust security, compliance, and management features. It uses natural language to generate content, summarise documents, analyse data, and automate tasks in Word, Excel, Outlook, PowerPoint, and Teams. It has a conversational interface that allows users to interact with their work data and documents using AI-powered chat. You can build and manage custom AI agents tailored to your business needs, including SharePoint-based agents and integrations via Microsoft Graph connectors. It has built in data protection, IT management controls, and compliance with Microsoft's enterprise security standards. Copilot reasons over personal work data (emails, files, meetings) to provide context aware assistance.	23/05/2025	CISO/HoDI
STAFF CAN USE THESE TOOLS BELOW, BUT MUST NOT UPLOAD MINISTRY DATA INTO THE AI SYSTEMS			
Adobe Express	Adobe Express is a user-friendly, web-based content creation platform designed for anyone—from beginners to	23/05/2025	CISO/HoDI

	professionals—who wants to quickly create high-quality graphics, videos, and documents. It's especially popular among social media marketers, educators, small businesses, and content creators.		
Adobe Sensei	Adobe Sensei is Adobe's AI engine that powers smart features across its apps to help users create, edit, and analyse content more quickly and intelligently. It is generally built into other Adobe products such as photoshop and lightroom rather than being an app in itself.	23/05/2025	CISO/HoDI
ChatGPT	ChatGPT is based on a large language model (like GPT 4), trained on vast amounts of text data. It doesn't "know" things like a human does, but it can generate highly relevant and coherent responses based on patterns in the data it was trained on.	23/05/2025	CISO/HoDI
Anthropic Claude	Anthropic Claude is a family of advanced AI models developed by Anthropic, a company founded by former OpenAI researchers. As of 2025, the latest generation is the Claude 4 series, which includes two models: Claude Opus 4 and Claude Sonnet 4. These models are designed to be powerful, safe, and capable of handling complex, long-running tasks with minimal human input. It can: Understand and generate human like text, perform deep reasoning and analysis, automate workflows and long term tasks, write and debug code, summarise, search, and synthesise large volumes of information.	23/05/2025	CISO/HoDI
Google Gemini	Gemini (formerly Google Bard) is Google's conversational AI chatbot. Gemini runs on Google's family of multimodal AI models to understand and generate text, and work across other mediums like images, audio, and video.	23/05/2025	CISO/HoDI
Perplexity	Perplexity AI is an AI driven search engine and chatbot that uses large language	23/05/2025	CISO/HoDI

	models (LLMs) to answer user queries by drawing information from the web and providing cited sources within its responses. The AI model combines a traditional search engine with an AI assistant, delivering answers in natural language backed by references.		
Napkin AI	Napkin AI is a creative and organisational tool designed to help users capture, connect, and reflect on their ideas using artificial intelligence. It acts like a personal thinking partner, ideal for writers, researchers, creatives, and anyone who wants to make sense of scattered thoughts or inspirations.	23/05/2025	CISO/HoDI
NotebookLM	NotebookLM is a personalized AI research assistant that allows users to upload and organize their own content—such as PDFs, Google Docs, websites, and YouTube links—and then interact with that content using natural language. It's powered by Google's Gemini AI and is designed to help users transform complex information into actionable insights.	28/07/2025	CISO/HoDI
*** CISO/HoDI = Chief Information Security Officer | Head of Data & Insights**			