Ministry for the
Environment
Manatū Mō Te Taiao

ORGANISATIONAL POLICY

Artificial Intelligence (AI) Use Policy

The Artificial Intelligence (AI) Use Policy provides guidelines for the responsible and trustworthy use of AI in Manatū Mō Te Taiao, Ministry for the Environment.

Contents

Policy Owner, Sponsor and Review dates

Policy owner	GM Information Technology
Dep Sec Sponsor	Laura Dixon Deputy Secretary Business Transformation and Services
Next review	31 December 2025 and annually thereafter

Expectations of public servants

As public servants, we are expected to act with a spirit of service to the community, upholding the public service values:

- **Impartial** – treat all people fairly, without personal favour or bias
- **Accountable** – take responsibility and answer for work, actions and decisions
- **Trustworthy** – act with integrity and be open and transparent
- **Respectful** – treat all people with dignity and compassion and act with humility
- **Responsive** – understand and meet people's needs and aspirations.

This policy helps us live up to these values.

Purpose

The Artificial Intelligence (AI) Use Policy provides guidelines for the responsible and trustworthy use of AI at Ministry for the Environment (MfE). It is designed to ensure that we can benefit from AI while staying aligned with our information management principles, managing the potential risks and ensuring compliance with New Zealand government statutory and legislative requirements, particularly around data protection and privacy.

MfE defines AI and AI tools as:

- Automation – augmentation of human workers with digital works to streamline business processes
- Inference – running live data through a trained AI model to make a prediction or solve a task
- Generative – submitting a prompt into an AI tool to generate new content.

Search engines such as Google and other tools of an earlier variant are not covered by this policy but must still be approved for use.

Who is covered by the policy

This policy applies to all employees, contractors and third parties who use or have access to AI and access MfE's digital environment. This policy will apply to core third-party ICT contractors and vendors who use or have access to MfE's data within their systems or when they apply results from AI to MfE's systems.

Principles

MfE is following the advice and guidance from the Government Chief Digital Officer, the Government Chief Data Steward, and the Government Chief Information Security Officer. We are also informed by the New Zealand Privacy Commissioner's guidance as outlined in 'Artificial Intelligence and the Information Privacy Principles'[1].

They key principles are:

- **Use only Approved AI Tools for classified information**: Only AI tools approved by MfE's Chief Information Security Officer, as listed on Te Taiao, are permitted to be used with classified information (i.e. information classified as IN-CONFIDENCE). This will ensure that the security and terms associated with the use of a tool are understood.
- **Protect Confidential Information**: Ensure that no information classified SENSITIVE or above or personal information is inputted into these tools, and all AI usage must comply with the Privacy Act 2020 and the Official Information Act 1982.
- **Ensure Accuracy and Transparency**: Conduct accuracy checks on AI-generated responses to avoid factual errors, biases, or inappropriate content. Declare the use of AI in any externally published or presented work, including relevant copyright information, references, and acknowledgements.
- **Respect Māori Data and Perspectives**: Engage with Te Tiriti partners when Māori data or interests are involved. Understand the context and implications of AI use for Māori, including considerations of whakapapa, mātauranga, tapu, taonga, and Māori data governance and sovereignty.

Policy statements

AI can enhance productivity, creativity, and efficiency, but it needs to be used responsibly, ensuring the protection of information. This policy sets out the guidelines for using AI tools at MfE. When using AI tools at MfE, you must adhere to the following guidelines that underpin the principles:

- **Compliance with this policy:** If you fail to comply with this policy, it may be considered a breach of our Code of Conduct and as a result may lead to disciplinary action being taken.

- **Approved AI tools:** You can only use AI tools that have been approved by MfE's Chief Information Security Officer to process classified information (i.e. information classified as IN-CONFIDENCE). The list of approved AI tools is published on Te Taiao and regularly updated. Unapproved tools can be used with unclassified information.

- **Ensure accuracy**: An accuracy check must be carried out for any responses provided by AI as these responses can contain factual errors, biases, or inappropriate content. Always check validity and content of any AI output.

- **Ensure transparency:** You must declare if AI is used in work that is published or presented externally. This should be included with any copyright information, references, and acknowledgements.

[1] Artificial intelligence and Information Privacy Principles, Privacy Commissioner, AI-and-the-Information-Privacy-Principles.pdf

- **No personal information:** Do not share, or input data like passwords, credit card numbers etc. This includes any personal information like names, addresses, phone numbers etc.
- **No information above IN-CONFIDENCE:** No information classified as SENSITIVE or above is to be shared or input into AI tools. This means only information deemed up to and including IN-CONFIDENCE can be input into approved AI tools.
- **Privacy Act 2020:** All usage of AI must adhere to the 13 principles in the Privacy Act 2020.
- **Official Information Act 1982:** Remember that any use of AI may be subject to discovery under the Official Information Act.
- **Taonga of data:** Māori representatives have expressed varying views, some strongly held, about government use of AI tools. You should work with our relevant Te Tiriti partners if Māori data is involved or where Māori interests or outcomes could be affected through the use of AI. You should also understand important context for Māori and the Crown, including why AI is being considered, how it could impact Māori and services to Māori, what Māori data might be involved and its status with regards to key cultural concepts such as whakapapa, matauranga, tapu and taonga, and how Māori data governance[2] and sovereignty might apply.
- **3rd party contractors/vendors:** 3rd party contractors/vendors providing a product and/or service to MfE, or are procuring such services from a supplier, are required to adhere to MfE policies and procedures including this AI Use Policy.

Key accountabilities and responsibilities

Role	Responsibility/Accountability
Governance and Oversight	
Deputy Secretary Business Transformation Services (Chief Operating Officer, Chief Security Officer)	• Sponsor of this policy
General Manager Information Technology (Chief Information Officer, Chief Information Security Officer)	• Owner of this policy • Has overall oversight of the use of AI at MfE • Approves which AI tools are permitted to be used within MfE • Approves future changes and annual renewal of policy • Accountable for leading the development, promotion, and embedding of MfE's AI capability and culture.
Te Mīmiro	• Approves the initial policy (V2.0) prior to socialisation • Ensures policy meets MfE's operational needs balancing risk and enablement
Business Groups: Identify and manage risks in day-to-day operations (1st Line)	

[2] TE KĀHUI RARAUNGA, MĀORI DATA GOVERNANCE MODEL, b8e45c_a5b7af8b688c4cd9b7583775c27da52e.pdf

Role	Responsibility/Accountability
Deputy Secretaries (Dep Secs)	• Provide leadership to embed policies and procedures in their business group • Ensure their business group is compliant with policies and procedures
All Managers	• Accountable for their people's usage and access to approved AI tools
All Staff	• Usage of AI tools under the Acceptable Usage policy, and all content that is input by them and received from the AI tools they use.
Risk Oversight Functions: Setting policies and monitoring compliance (2nd Line)	
IT Security Manager	• Monitor usage and provide advice to staff to ensure that this policy is followed • Identifies and reports significant risks and issues to the CISO and governance • Ensures this policy is working effectively through regular monitoring and reporting of policy compliance
Privacy Officer	• Advice on policy with respect to privacy issues arising from the use of AI tools.
AI Working Group	• Review AI business cases and make prioritised recommendations to Te Mīmiro on their implementation. • Make AI-related IT investment considerations and make recommendations to Te Mīmiro for approval (in the context of the Ministry's investments in IT as a whole) • Identify and mitigate ongoing AI risk, including through appropriate policies, controls, and staff education initiatives • Undertake/make recommendations on new AI guidance and information from the public service • Ensure that Te Ao Māori is embedded in AI governance approaches.
Independent Assurance (3rd line)	
Internal Assurance	• Provide independent assurance over the design and operation of governance, risk management and internal controls, including 1st and 2nd lines
Audit and Risk Committee	• Provide recommendations, assurance and advice to the CE on the effectiveness of governance practices, risk management, internal controls and management assurance activities

Relevant legislation, regulations and standards

This policy has been created in response to the Interim Generative AI guidance for the public service, published on digital.govt.nz, on 26 July 2023. This policy is also governed by the following:

- MfE's Information Systems Acceptable Use Policy
- Information Management Policy

- Public Services Commission Standards of Integrity and Conduct.

See the following Acts for more information:

- Privacy Act 2020
- Official Information Act 1982.

Measures of success and compliance management

The GM IT will assess the effectiveness of this policy. The following measures of success outline what we expect to see if the policy is working:

- Usage of unapproved tools decreases (<10% of AI tool users are using unapproved tools)
- The channel for raising requests to the AI Working Group is understood.
- Percentage of contractors and third parties declaring their use of AI in work completed for MfE

The GM IT will monitor compliance with this policy as follows:

- AI tool usage will be reported on monthly, and people identified using unapproved tools are communicated with.

Non-compliance

Failure to comply with this policy may be considered a breach of the Code of Conduct.

Additional Guidance

The list of Approved AI Tools is on the Technology page of Te Taiao and will be regularly reviewed.

If you have any questions or need support in relation to the use of AI tools, please contact ITSecurity@mfe.govt.nz

Department of Internal Affairs: Initial advice on Generative Artificial Intelligence in the public service (July 2023) *Joint guidance from data, digital, procurement, privacy and cyber security system leaders*

Office of the Privacy Commissioner: Artificial Intelligence and the Information Privacy Principles (Sept 2023) *How to use AI tools to ensure obligations are met under the Privacy Act 2020*

NZ National Cyber Security Centre: Engaging with Artificial Intelligence (Jan 2024) *Joint guidance from NCSC, Australian Cyber Security Centre and 12 other international cyber security agencies on how to use AI systems securely.*

Document History

Name	Role	Version	Date	Comments
Chris Warne, Lynn Court	Security & Risk Analyst, Senior IT Business Analyst	0.1	26/02/2024	Initial draft
Kelsi Loader	Senior IT Project Manager	0.2	08/03/2024	Reviewed
Steven Wheeler, Leon Sullivan Elias Wyber	IT Security Manager, IT Operations Manager, Programme Director Data & Reporting	0.3	12/03/2024	Reviewed
Lynn Court	Senior IT Business Analyst	0.4	13/03/2024	Updated with review comments from 12/03/24
Duncan Stuart & Sam Palaroan	Risk Assurance & Resilience	0.5	13/03/2024	Reviewed
Lynn Court	Senior IT Business Analyst	0.6	14/03/2024	Updated with review comments from 13/03/24
Lynn Court & Gemma Seddon	Senior IT Business Analyst IT Project Delivery Manager	0.7	15/3/2024	Reviewed and updated for final IT Managers review
Steven Wheeler, Leon Sullivan Elias Wyber	IT Security Manager, IT Operations Manager, Programme Director Data & Reporting	0.8	19/03/2024	No additional comments added from this review. Doc prepared for review by General Manager
Mike Porter	General Manager, Information & Technology/Chief Information Security Officer	0.9	22/03/2024	Reviewed
Kelsi Loader	Senior IT Project Manager	1.0	04/09/2024	Final version, confirmed with Steven Wheeler (IT Security Manager)
Steven Wheeler Lynn Court	IT Security Manager Senior Business Analyst IT	1.01	19/11/2024	Re-aligned with prior approved wording post transfer to new Risk team's template.
Steven Wheeler	IT Security Manager	2.0	03/12/2024	Incorporated feedback from COO and Risk and Assurance Manager.

Steven Wheeler	IT Security Manager	3.0	01/07/2025	Raised classification level for approved AI tools to IN-CONFIDENCE