

5 May 2026

s9(2)(a)

Mālō e lelei s9(2)(a),

## RESPONSE TO AN OFFICIAL INFORMATION ACT REQUEST (REF: DOIA036-2025/26)

On 3 April 2026, you contacted the Ministry for Pacific Peoples (the Ministry) requesting under the Official Information Act 1982 (OIA), information relating to internal digital infrastructure, cloud services and AI tools. I have outlined your specific request and my response below.

*I am conducting academic research into New Zealand's reliance on overseas digital infrastructure and AI services, and the implications for New Zealand's sovereignty and decision-making independence. I have made a separate parallel request to MBIE regarding All-of-Government (AoG) procurement arrangements. This request is focused on each agency's own internal arrangements, documents, and policies.*

*For each agency receiving this request, please provide the following documents:*

### 1. Core Productivity and Email platform

- Any contract, licence agreement, or service agreement between your agency and a provider of productivity or email software (e.g. Microsoft 365, Google, Workspace, or other), including any schedules specifying term dates.
- If procured through an AoG arrangement, any agency-level order form, call-off agreement, or accession document relating to that arrangement.

The Ministry uses Microsoft (MS) 365 as its core productivity and email platform. Licensing is obtained through a managed service contract established in accordance with the All-of-Government (AoG) procurement frameworks and guidelines, including Government Marketplace.

Information relating to this managed service arrangement, including detailed contractual terms, licensing conditions, schedules, pricing, service arrangements, and any agency-level order forms or call-off documentation, is commercially sensitive. This information is therefore withheld under section 9(2)(b)(ii) of the OIA, as making it available would be likely to unreasonably prejudice the commercial position of the parties to whom the information relates.

#### Auckland

9 Ronwood Ave, Manukau  
PO Box 97005,  
South Auckland Mail Centre 2240  
P: 09 265 3200

#### Wellington National Office

Level 7, 1 Bowen House  
Wellington, 6011  
PO Box 833, Wellington 6143  
P: 04 473 4493

#### Christchurch

Level 1, BNZ Centre  
120 Hereford St  
Private Bag 4741,  
Christchurch 8011

In accordance with section 9(1) of the OIA, the Ministry has considered the public interest in the release of this information and has determined that, in this instance, the need to withhold commercially sensitive information outweighs any public interest in disclosure.

- *Any internal documents specifying data residency or data sovereignty requirements in connection with your productivity platform.*

The Ministry does not maintain standalone MS 365-specific data residency documents. I am refusing this part of your request under section 18(e) of the OIA as the information requested does not exist.

## 2. Cloud Infrastructure and Storage

- *Any contract, licence agreement, or service agreement between your agency and a cloud infrastructure or storage provider (e.g. Amazon Web Services, Microsoft Azure, Google Cloud), including any schedules specifying term dates.*

The Ministry operates a cloud-first environment as part of its managed service operating model. Cloud Services are delivered through our managed service arrangement, with procurement conducted in accordance with AoG procurement guidelines. Specific details of the management service contract are commercially sensitive and therefore withheld under section 9(2)(b)(ii) of the OIA.

- *Any security assessment, risk assessment, or privacy impact assessment produced in connection with the use of any cloud infrastructure provider.*

Cloud-related risks are managed through the Ministry's standard information security, privacy and assurance processes, which apply across all ICT services. These processes are aligned with Protective Security Requirements and Government Digital Delivery Agency (GDDA) guidance. The individual assessment documents include commercially sensitive and security-related information relating to system configurations and are therefore withheld under section 9(2)(b)(ii) of the OIA.

- *Any internal documents specifying data residency or data sovereignty requirements in connection with cloud infrastructure.*

The Ministry does not maintain standalone MS 365-specific data residency documents. I am refusing this part of your request under section 18(e) of the OIA as the information requested does not exist.

## 3. AI Tools and Internal AI Policy

- *Any contract, licence agreement, or service agreement between your agency and a provider of AI tools or services (e.g. Microsoft Copilot, any OpenAI-based product, Google Gemini, or similar), including the provider name, general purpose, and any schedules specifying term dates.*

The Ministry uses the standard MS Copilot capability provided as part of the MS 365 E5 licensing model, delivered through a managed service arrangement. The Ministry does not hold any separate or standalone contracts with AI tool providers, including OpenAI-based services, outside

of this arrangement. The information includes commercially sensitive and contractual details, such as licensing terms and schedules, and is therefore withheld under section 9(2)(b)(ii) of the OIA.

- *Any internal policy, guideline, or usage framework document relating to the use of AI tools by your agency's staff, including any approved or preferred provider lists.*

The Ministry has a Generative Artificial Intelligence (GenAI) Tools Guideline that supports safe and responsible AI use. The guideline aligns with the GDDA Public Service AI Framework and reflects the Ministry's people-centred and trust-based operating model. The guideline has been appended to this letter.

- *Any risk assessment, privacy impact assessment, or security assessment produced in connection with the adoption or use of AI tools at your agency.*

Risk, privacy and security assessments have been completed for the enablement of MS Copilot within the Ministry's MS 365 programme. These assessments consider security, privacy, and appropriate use controls and are overseen by the Ministry's Information Privacy & Security Governance group. Specific assessment documentation contains commercially sensitive and security-related information concerning system configuration and is therefore withheld under section 9(2)(b)(ii) of the OIA.

In line with standard OIA practice, the Ministry proactively publishes some of its responses to OIA requests. As such, this letter may be published on the Ministry for Pacific Peoples' website. Your personal details will be removed, and the Ministry will not publish any information that would identify you or your organisation. Should you wish to discuss this response with us, please feel free to contact the Ministry at: [ويا\\_requests@mpp.govt.nz](mailto:ويا_requests@mpp.govt.nz).

If you are dissatisfied with this response, you have the right, under section 28(3) of the OIA, to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at [www.ombudsman.parliament.nz](http://www.ombudsman.parliament.nz) or freephone 0800 802 602.

Mālo 'aupito,



Mauailegalu Mathew So'otaga  
Acting Deputy Secretary  
**Corporate & Support Services**

Ministry for Pacific Peoples

# Use of Generative Artificial Intelligence (GenAI) Tools

Guidelines

Deputy Secretary, Corporate & Support Services

April 2024

## Document

This document contains the guidelines for the use of Generative Artificial Intelligence (AI) tools at the Ministry for Pacific Peoples (MPP).

## Version History

| VERSION | DATE           | AUTHOR                              | KEY CHANGES                                                                                                                         |
|---------|----------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | 05 April 2024  | Kate Brewer                         | First draft                                                                                                                         |
| 2.0     | 24 April 2024  | Kate Brewer                         | Updated based on feedback (Transitional Director IT, Director Operations Corporate Services, Principal Advisor Risk and Assurance). |
| 3.0     | September 2020 | Principal Advisor, People & Culture | Annual review and amendments                                                                                                        |
| 5.0     | December 2024  | Director, People & Capability       | Updated in line with legislation. Procedural aspect moved to guidelines                                                             |

**Note:** Do not make unauthorised electronic copies or new versions (drafts) of this corporate policy. Contact the Director, People and Capability to have new drafts initiated and recorded in the appropriate manner.

## Status

|                |                                               |
|----------------|-----------------------------------------------|
| CONTACT        | Chief Information Security Officer            |
| STATUS         | In effect from May 2024                       |
| APPROVED DATE  | May 2024                                      |
| POLICY OWNER   | Ministry for Pacific Peoples                  |
| BUSINESS OWNER | Deputy Secretary Corporate & Support Services |
| REVISION CYCLE | Every two years or as needed                  |
| NEXT REVIEW    | December 2025                                 |

## Signoff

| NAME                     | ROLE                                           | SIGNATURE                                                                            | DATE            |
|--------------------------|------------------------------------------------|--------------------------------------------------------------------------------------|-----------------|
| Danilo Coelho de Almedia | Deputy Secretary, Corporate & Support Services |  | 3 December 2024 |

## Table of Contents

---

|                                        |   |
|----------------------------------------|---|
| 1. Introduction .....                  | 4 |
| 2. Guidance Principles .....           | 4 |
| 3. Why do we need a GenAI Guide? ..... | 5 |
| 4. Benefits of GenAI .....             | 5 |
| 5. Risks of GenAI .....                | 5 |
| 6. Definitions .....                   | 6 |
| 7. Further Resources .....             | 6 |





## 1. Introduction

This document sets out MPP's expectations on the responsible use of Generative Artificial Intelligence (GenAI) at MPP.

MPP has undertaken an IT Security Assessment of Microsoft's Co-pilot GenAI tool.

### **MPP'S CURRENT POSITION IS:**

- **Co-pilot has been approved as MPP's enterprise GenAI tool;**
- **MPP staff can use Co-pilot in accordance with the Guidance Principles below;**
- **Use of any other GenAI tool is not permitted without an IT Security Assessment and approval from MPP's Chief Security Officer, Chief Information Security Officer and Chief Privacy Officer; and**
- **Personal or sensitive information must not be inputted into Co-Pilot AI tool.**

## 2. Guidance Principles

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Don't use Co-pilot for any MPP data classified as SENSITIVE or above                                | The risks for security and potential impacts if Government SENSITIVE or above datasets were to be compromised could be extremely serious. Do not input these types of datasets into Co-pilot.                                                                                                                                                                                                                                                                                                                                                                     |
| Don't input personal information into Co-Pilot                                                      | In situations where it isn't possible to use non-personal information, a Privacy Impact Assessment must be conducted, all potential risks must be identified and addressed, and the Assessment must be approved by MPP's Chief Privacy Officer.                                                                                                                                                                                                                                                                                                                   |
| Don't use any other GenAI tool                                                                      | This could create a risk of technologies being used in ways that could result in privacy or security breaches or disrupt the organisation's current and approved technology environment. If staff require use of an AI tool other than Co-pilot, an IT Security Assessment must be conducted, and approval of the tool must be provided by MPP's Chief Security Officer, Chief Information Security Officer and Chief Privacy Office. A Privacy Impact Assessment may also need to be conducted if the tool is intended to be used to input personal information. |
| Don't input any information into Co-Pilot that would be withheld under the Official Information Act | The risks for the integrity of the public service and potential impacts if redacted information were to be accessed and or inappropriately used could be extremely damaging for public trust and confidence.                                                                                                                                                                                                                                                                                                                                                      |
| Don't use Co-pilot for Ministry decision-making processes.                                          | MPP is required to understand its own decision-making processes and to be able to explain those decisions when questioned to do so. Using GenAI for essential systems and services uses AI algorithms which are extremely complex to understand and very difficult to explain how the output was reached.                                                                                                                                                                                                                                                         |

### 3. Why do we need a GenAI Guide?

---

- GenAI, when used appropriately, can improve services provided by organisations and Government agencies. GenAI is currently being integrated into cloud, security and other services around the world and so is no longer something organisations can or necessarily should avoid using.
- However, New Zealanders have concerns about the use of AI, and they have expectations that any use of it by Government agencies will be done so carefully, ethically and securely.
- This guidance is intended to support staff at MPP to understand the benefits and risks and to be aware of the Ministry's expectations regarding the proper use of the approved GenAI tool, Co-pilot.

### 4. Benefits of GenAI

---

- AI assists with mechanical and tedious tasks (i.e. counting or data matching) that people might not want to or be able to do. Those tasks are likely better suited to automation such as offered by AI tools.
- AI can save time. GenAI can be used to create a first draft of documents, but the GenAI outcomes are limited in their ability to create new critical content, and any output requires careful review.
- By using algorithms AI can detect patterns in large volumes of data and can interpret their meaning. Analytics created by AI in this way can use and access more data, are more detailed, and the models improve over time.

### 5. Risks of GenAI

---

- As AI models are created off training data which is often publicly sourced or sourced from the input of others using the AI tool, information specific to minority groups may not be well represented in the data drawn from the AI tool and results can be discriminatory or unfair.
- Inputting personal or sensitive information into the AI model without consent or authority may lead to a privacy and / or security breach by the organisation.
- Hackers may manipulate AI models to facilitate cyber-attacks. AI tools can be used to impersonate real people, create fake identities and to assist with online hacking and phishing scams.
- Some AI tools can leak sensitive information that increases security risks. AI models have been known to suggest real passwords.
- AI makes it easier to exploit illegally obtained information from data breaches, to re-identify people in published datasets, and to combine any sources of data to build detailed profiles of people which are more or less accurate.
- Poorly considered prompts used in the AI model may lead to inaccurate responses from it.



## 6. Definitions

| TERM                        | DEFINITION                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Artificial Intelligence     | AI is software that learns from data. AI tools are built on 'training data' (see definition below) and examples of AI tools include software used to review and summarise legal documents using language matching; the predictive text function on your laptop or phone; and content creating tools (see definition below) such as Co-pilot.                                                                    |
| Generative AI               | Is one type of Artificial Intelligence technology that can produce content – such as text, images or audio – by matching the prompts or questions it receives to patterns in the data that it has. On the basis of probability, the technology then uses that matched data to 'fill in the blanks' and create or generate text or images that closely resemble human-related content.                           |
| Publicly available AI tools | These sit outside an agency's own environment as third-party AI platforms or software. Apart from Microsoft's Co-pilot, these tools have not been risk assessed by MPP to the standard expected for NZ Government agencies. Open AI's ChatGPT, Microsoft's Bing search and Google's Bard are the most well-known examples of free and publicly available GenAI.                                                 |
| Personal Information        | Information about a living individual. Examples include a person's name, telephone number, address, date of birth, ethnic origin and financial information. Even if a person's name is not recorded, but there is a reasonable chance that they could be identified from other information or a combination of pieces of information, it can still be personal information for the purposes of the Privacy Act. |
| Training data               | is an extremely large dataset that is used to teach machine learning models of AI. The data is often publicly sourced or sourced from the input of others using the AI tool and can take various forms, such as images, audio, or text.                                                                                                                                                                         |

## 7. Further Resources

- [Privacy Policy.docx](#)
- [Privacy Act 2020](#)
- [Summary of Guidance from Office of Privacy Commissioner on GenAI.docx](#)
- [Office of the Privacy Commissioner | Generative Artificial Intelligence.](#)
- [Interim GenAI guidance for the public service — Full guidance \(PDF 193 KB\)](#)
- [Interim GenAI guidance for the public service — Summary \(PDF 230 KB\)](#)

*This document is a first effort by MPP to provide help to staff to use this new class of technology. It will be updated as the technology evolves, and the risks and impacts are better understood.*