DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

18 August 2026

Ref: OIA-2026/27-0054

[redacted]

Tēnā koe [redacted],

Official Information Act request: Māori data governance, AI tools, and automated decision-making

Thank you for your Official Information Act 1982 (the Act) request, which was received by the Department of the Prime Minister and Cabinet (DPMC) on 21 July 2026. You requested:

> *"Following on from my 2024/25 OIA request and successful publication of results; I am seeking an update to my original request for any updates from your original response (up to the date of this request), and a new section of questions relating to Artificial Intelligence and Algorithms.*
>
> *Requested 2026 updates if any, from my previous OIA to the date of this request:*
> 1. *How does your organisation define Māori data as opposed to non-Māori data?*
> 2. *Does your organisation have Māori Data Sovereignty and or a Māori Data Governance policy or strategy? If yes, I request a copy.*
> 3. *I also request a copy of your organisation Data Governance strategy/policy/policies?*
> 4. *Has your organisation had with any success or no/limited success, implementation of any Māori Data Sovereignty Principles or Māori Data Governance? If yes, please provide details of the implementation and how you measured its success.*
> 5. *How many fte are allocated to Māori Data practices in your organisation?*
> 6. *What country/countries are the majority of your organisation's data stored?*
> 7. *Which Cloud Provider(s) do you use?*
>
> *New requests:*
> 8. *A list of all artificial intelligence systems, machine learning models, and automated decision-making (ADM) tools currently in use, in procurement, or in pilot within the agency, including the name, purpose, vendor/developer, and date of deployment of each.*
> 9. *A list of all generative AI tools approved for staff use, and copies of any internal policies or guidance governing staff use of generative AI.*
> 10. *Copies of all Te Tiriti o Waitangi analyses, assessments, or advice prepared in relation to any AI or ADM system in use or in development, including the identity of who prepared them.*
> 11. *Records of any engagement, consultation, or partnership with iwi, hapū, or Māori organisations regarding the design, procurement, deployment, or governance of AI or ADM systems, including dates, parties, and outcomes.*
> 12. *Any documents identifying whether Māori data (including data about Māori individuals, whānau, hapū, iwi, or mātauranga Māori) is used to train, fine-tune, test, or operate any AI system, and any governance arrangements applying to that data.*
> 13. *Copies of any advice, briefings, or policies referencing Māori data sovereignty, Māori Data Governance, or WAI 2522 in relation to the agency's AI or ADM systems.*

Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9698 www.dpmc.govt.nz

14. Copies of all Privacy Impact Assessments, Algorithmic Impact Assessments, human rights assessments, or equity analyses completed for any AI or ADM system, including any assessment of differential impacts on Māori."

For ease of reference, I have renumbered the parts of your request.

The Central Agency Shared Services (CASS), hosted by The Treasury, delivers internal operational support (IT, information management, finance and payroll support) to DPMC and the Treasury. Ordinarily, insofar as your request concerns information more closely connected to or held by CASS, I would partially transfer your request to the Treasury. However, I understand that you have made your request directly to that agency. I instead refer you to their forthcoming response.

Parts 1 to 7
Our answers to these parts of your request remain unchanged from those provided in our previous response (OIA-2024/25-0520 refers). For Parts 6 and 7, I also refer you to the forthcoming response from the Treasury, which will cover any additional information relevant to the services provided to DPMC by CASS.

Parts 8 and 9
DPMC does not use automated decision-making tools or machine learning models; nor are any such tools or models being piloted. All DPMC staff have access to two AI tools: Paerata, which was developed by the Treasury, and Microsoft 365 (M365) Copilot Chat Basic, developed by Microsoft. DPMC is also currently piloting M365 CoPilot (licensed) and ChatGPT Enterprise.

<table>
<tr><th>AI Tool</th><th>Vendor/ developer</th><th>Date available to DPMC staff for use</th><th>Purpose</th></tr>
<tr><td>Paerata</td><td>CASS, The Treasury</td><td>December 2024</td><td rowspan="2">To support day-to-day work, including drafting emails and documents, summarising information, and assisting with research and general queries.</td></tr>
<tr><td>M365 CoPilot Chat Basic</td><td rowspan="2">Microsoft</td><td>April 2026</td></tr>
<tr><td>M365 CoPilot</td><td>1 July 2025</td><td rowspan="2">DPMC is trialling both ChatGPT Enterprise and M365 CoPilot licences to assess the value of generative AI in supporting knowledge work across drafting, research, information synthesis, and productivity tasks within core business tools. Use is governed by DPMC's AI policy and guidance to ensure responsible use, human oversight, and appropriate information handling.</td></tr>
<tr><td>ChatGPT Enterprise</td><td>Open AI</td><td>1 July 2025</td></tr>
</table>

In addition to the information above, I have identified the documents listed in the table below as relevant to Part 9 of your request and have decided to release these to you:

Item	Date	Document description	Decision
1	April 2026	Policy	Release
2	April 2026	CoPilot Basic Guidance	Release

DPMC's Paerata User Guidance and Gen-AI User Guidance are also relevant to Part 9 of your request. This part of your request is refused under section 18(d) of the Act, as these documents are publicly available at: https://www.dpmc.govt.nz/sites/default/files/2025-08/dpmc-roia-oia-2024-25-1001.pdf.

Parts 10 to 13
DPMC has not identified any information within scope of these parts of your request. I am therefore refusing these parts of your request under section 18(e) of the Act, as the information requested does not exist.

Part 14
The privacy assessment for Paerata was completed by the Treasury, which developed the tool. It is publicly available here as 'Document 3':
https://www.treasury.govt.nz/sites/default/files/2025-11/oia-20250740.pdf

A DPMC privacy assessment for a specific use case of Paerata may also be relevant to this part of your request and is publicly available here:
https://www.dpmc.govt.nz/sites/default/files/2025-12/dpmc-roia-oia-2025-26-0263.pdf.

These documents are refused under section 18(d) of the Act.

Finally, DPMC is currently preparing a Privacy Impact Assessment for M365 CoPilot and ChatGPT Enterprise. As the assessment remains in draft and is still subject to internal consideration, I have decided to withhold it in full under section 9(2)(f)(iv) of the Act, to maintain the confidentiality of advice tendered by or to Ministers and officials, and section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between officials. To the extent the draft assessment contains legally privileged material, I have also withheld that information under section 9(2)(h), to maintain legal professional privilege.

In making my decision, I have considered the public interest considerations in section 9(1) of the Act. No public interest has been identified that would be sufficient to outweigh the reasons for withholding that information.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the DPMC website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Nāku noa, nā



Michelle Menken
Acting Deputy Chief Executive, Corporate and Chief People Officer

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

DPMC Artificial Intelligence Policy

iManage reference	4968101	**Date approved**	9/04/2026
iManage version	2.0	**Contact**	Deputy Chief Executive Corporate and Chief People Officer
Approved by	Chief Executive, DPMC	**Name** **Signature**	Ben King 
Date amended version approved	N/A	**Date for review**	October 2026 This policy will be regularly reviewed a minimum of every 6 months and updated to reflect new technological developments. The field of AI is rapidly evolving, and regular reviews ensure that the policy remains relevant and effective. This includes incorporating new best practices, addressing emerging challenges, and updating guidance as needed.

Policy Overview and Objective

1. The Department of the Prime Minister and Cabinet's (DPMC) vision is to be a system leader in Artificial Intelligence (AI) adoption across the New Zealand government. This includes a strategic outcome for DPMC's AI adoption to foster a proactive, future-focused organisation where staff confidently use AI to enhance their work, innovate boldly and operate within clear and trusted safeguards.

2. This AI Policy supports our AI transformation work programme to build a confident and capable workforce at DPMC that leverages AI to create efficiencies, streamline processes, and enhance decision making.

3. The policy operationalises this vision to accelerate our use of AI technology in a responsible, ethical and safe manner, while balancing the benefits of AI innovation and maintaining security and safety by mitigating potential risks.

Released under the Official Information Act 1982

4. This policy sets out principles, responsibilities and processes for developing, adopting and using AI tools and follows guidance set out in the Public Service AI Framework and Responsible AI Guidance for the Public Sector.

5. This policy must also be read with the DPMC IT and Acceptable Use Policy and specific guidance for each approved tool.

Policy Statement

6. DPMC will:

   a) leverage AI to improve efficiency and productivity, enhance policy and service design and delivery, and foster innovation,

   b) harness the benefits of AI innovation while mitigating potential risks to maintain security and safety,

   c) adhere to the approach set out in this policy to support the responsible and safe use of AI within DPMC, and

   d) provide staff with appropriate training and clear guidance on the appropriate use of approved AI tools.

Use of AI tools

7. Staff must only use approved tools enabled on DPMC work devices for work purposes.

8. Staff should make themselves aware of what AI enabled tools and applications are approved for use 'on the whitelist', and what tools are set out on the 'blacklist' (as updated on the AI page on Kāinga).

9. All tools and applications enabled on work devices with activated AI features, are approved for use. For example, this includes Google Chrome, Microsoft Co-Pilot Chat (Basic), Microsoft Edge, and Adobe.

10. When using approved AI tools staff must follow appropriate guidance associated with using each AI approved tool and must not:

    a) enter DPMC information[1] above the appropriate classification standard required in the guidance for that approved tool,

    b) enter any information in breach of the Protective Security Requirements and IT and Communication Technology Acceptable Use Policy

Released under the Official Information Act 1982

[1] 'DPMC information' refers to information you only have access to by virtue of your employment at DPMC.

c) input commercially sensitive, legally privileged material (without the approval of the Chief Legal Advisor), or intellectual property information, unless guidance for the approved tool specifies otherwise,

d) enter personal information, including their own, unless it's already publicly available or a decision has been taken to allow the use of personal information under a privacy impact assessment, and the user guidance for that tool is clear that it can be used.

14. When producing a DPMC output using AI tools staff should take into account:

a) AI tools should not replace human input. AI tools must not materially contribute to decisions that could lead to an adverse outcome for an individual such as determining a response to a request or complaint, assessing an application for a service or document, or any other interaction where discretion is exercised.

b) Prompts inputted or outputs generated by AI in the course of conducting DPMC's related work are official information and need to be treated accordingly in line with the DPMC Information Management Policy and the Public Records Act 2005.

Audience and application

15. This policy should be applied by all DPMC staff when developing, approving, deploying or using AI technologies at DPMC. For the purposes of this policy, the term 'AI technologies' applies to all solutions, systems, applications, initiatives, and technologies (together referred to in this policy as 'tools') that offer or contain any degree of AI technology that may or may not be directly funded by DPMC.This policy applies to:

a) everyone in DPMC, including permanent, fixed-term, secondee, casual and agency temporary staff,

b) consultants and contractors including self-employed and independent contractors (together referred to in this policy as 'staff'), regardless of position or seniority.

17. Those involved in the procurement of products and services will consider how the prohibitions in paragraphs 15 will be appropriately reflected in contractual agreements.

18. Personal use of AI tools on personal devices is outside the scope of this policy.

Released under the Official Information Act 1982

Responsibilities

Role	Responsibilities
All DPMC People	All DPMC employees are responsible for using AI technology responsibly, lawfully, and in line with this policy.
DPMC's ELT Board	ELT Board is responsible for: • this AI Policy, • making the final decisions to approve all AI technology uses and tools within the DPMC, • granting exceptions to this policy (management override) only in exceptional circumstances, and, • ensuring the agency has appropriate policies and processes in place for the use of AI technology that reflect new developments, capabilities, and evolving ethical landscapes.
Tier 2 Leaders	Tier 2 Leaders are responsible for assuring the Chief Executive that their Business Group complies with departmental policies and processes relating to the use of AI
People Leaders	People Leaders are responsible for: • ensuring staff are aware of and compliant with this policy and other relevant corporate policies and guidance, • encouraging staff to build their skills in the use of AI tools, and ensuring any mandatory or relevant training is completed in a timely manner, and, • identifying issues and non-compliance of AI Policy and reporting these to the Corporate Group.
Staff	Staff are responsible for: • meeting the requirements of this policy and any associated policies, • complying with common law obligations (including duty to act fair and reasonably, and duty of care) and best practice, • adhering to relevant procedures, guidance, and attending any mandatory trainings, and, • identifying issues or non-compliance with this policy and reporting these to their People Leader.
DPMC Procurement	DPMCs Procurement lead is responsible for: • reviewing and approving third party provider contracts and ensuring appropriate compliance with this policy and any exceptions are made in line with guiding principles and safe and responsible use.

Released under the Official Information Act 1982

Role	Responsibilities
DPMC Legal	Responsibilities include: • DPMC's Privacy Officer is responsible for approving a privacy assessment for any requests to approve new AI tools or new uses of already-approved tools. DPMC's Privacy Officer is responsible for reporting on AI related privacy breaches, as appropriate.

Related policies, guidance, and information

19. This policy is underpinned and informed by:

- The Joint System Lead's Interim Generative AI Guidance for the Public Service
- the principles and rules of the Privacy Act 2020
- the Algorithm Charter for Aotearoa New Zealand
- the Digital Service Design Standard
- the Crown's commitments and obligations under Te Tiriti o Waitangi/Treaty of Waitangi, and
- the Government's Protective Security Requirements.

20. Other documents and policies that should be read in conjunction with this policy include:

- IT and Communications Technology Acceptable Use Policy (iManage 551779)
- DPMC and NEMA Gen-AI User Guidance on Kāinga
- Information and Records Management Policy (iManage 4795726)
- Privacy Policy on Kāinga
- Procurement Policy on Kāinga
- Protective Security Policy (iManage 4342432)
- Social Media Policy (iManage 4280517)

Released under the Official Information Act 1982

Definitions

Term	Definition
Artificial Intelligence	Is the field of computer science that seeks to create engineered systems that can generate outputs for particular sets of objectives without explicit programming.
DPMC information	Information you only have access to by virtue of your employment at DPMC.
Generative Artificial Intelligence	Technologies that can generate outputs for particular sets of objectives without explicit programming.
AI tools	Tools that can take input (sometimes through user input in the form of prompts or questions, but also in the form of existing text, documents, and images) and generate new or revised text or images that closely resemble human-created content. These tools work by matching user prompts to patterns in training data and probabilistically 'filling in the blank.' The term encompasses tools such as AI, Large Language Models, AI integrated tools, Machine Learning, Deep Learning, and any emerging factor-augmenting technologies.
Personal information	The Privacy Act 2020 defines 'personal information' as 'information about an identifiable individual'. This is a very broad definition, which covers information in hardcopy, electronic, verbal or any other form.

Released under the Official Information Act 1982

APPENDIX 1 – Principles guiding deployment of AI in DPMC

The following principles and considerations should be considered when adopting AI tools at DPMC.

Safety and security

a) Ensure privacy and security are paramount: All AI tools should be used, designed, and developed with privacy and security in mind.

b) Appropriate security controls and measures should be implemented to protect against cyber threats and unauthorised access or sharing of information. DPMC will implement robust measures to protect data privacy and ensure the security of AI systems.

Procurement

c) Staff involved in the procurement of AI tools will comply with DPMC Procurement Policy and the Government Procurement. This includes both entering contracts to procure an AI tool (contracts for services, statement of work etc.) as well as contracts with providers who are using AI in delivering services to DPMC (consultancy services order, contracts for services, etc.).

d) Before entering contracts to procure AI tools or contracts with providers who are using AI, staff must consult with CASS IT and the DPMC Legal Team regarding the nature and scope of those agreements.

Legal, regulatory and ethical context

e) Staff will ensure that the use of AI tools is compliant with relevant laws, regulations, and industry standards. Compliance with legal and regulatory requirements is essential to avoid legal risks and ensure that AI use aligns with broader societal standards and expectations.

f) This includes data protection laws, ethical guidelines, and industry-specific regulations. Regular audits and assessments should be conducted to ensure ongoing compliance.

Inclusive, sustainable development

g) DPMC AI systems and tools should contribute to inclusive growth and sustainable development through a focus on innovation, efficiency and resilience. Appropriate AI use at DPMC should consider equal access to technology, the treatment of inequality, and environmental impacts.

Human-centred values, ethics and transparency

h) New AI deployments and use case proposals should uphold democratic values and human rights, consider the appropriate disclosure of the use of AI, and how human oversight will be maintained to ensure ethical and appropriate use.

Released under the Official Information Act 1982

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Microsoft 365 CoPilot Chat (Basic) User Guidance

i-Manage reference	5152149	**i-Manage version**	1.0
Amended version approved by	Deputy Chief Executive, Corporate	**Name**	Alan Cassidy
Date approved	9/04/2026	**Date for review**	October 2026

Released under the Official Information Act 1982

Introduction

1. This document provides a guide for the safe, accurate and secure use of Microsoft 365 CoPilot Chat (Basic) (CoPilot Chat), which is now approved for use at the Department of the Prime Minister and Cabinet (DPMC).

2. CoPilot Chat is an AI assistant that is available to all DPMC staff on work devices as part of our corporate Microsoft 365 licence. It is integrated with the MS 365 ecosystem, aggregating data from SharePoint, OneDrive, Teams, and Outlook. Users can open the MS Copilot app to chat with a general virtual assistant or use MS Copilot to chat over documents or emails within Microsoft apps (like Outlook or Word).

3. This guidance should be read in conjunction with the DPMC Artificial Intelligence (AI) Policy and the IT and Communications Technology Acceptable Use Policy.

User Guidance

1. Use only approved tools

CoPilot Chat is approved for use at DPMC, issued under business licence and meeting DPMC security requirements. AI enabled tools and applications that are approved for use 'on the whitelist' are kept updated on the AI page on Kāinga.

2. Use CoPilot Chat in line with policies and guidelines

Staff must follow the appropriate guidance for each approved tool and become familiar with any exceptions relevant to each tool.

Staff should not use MS Co-Pilot Chat when working with sensitive personal information, or commercially sensitive, legally privileged, or third-party intellectual property (IP) information.

Staff should complete the Copilot Fundamentals module on eTipu before using CoPilot Chat – see further examples of when Copilot Chat should and shouldn't be used for DPMC work.

How can I use Copilot Chat at work?	When shouldn't Copilot Chat be used at work?
For simple explainers, such as explaining technical documents or concepts.	For tasks that have a personal nature. For example: • Assessing a colleague's performance. • Creating feedback on a staff member. • Ranking team members' capability. • Drafting comments for performance reviews or talent panels.
For summarising and comparing information.	For work involving information classified as SENSITIVE or RESTRICTED.
For coding.	When making decisions without applying a critical thinking lens and using your own judgement. For example: • Accepting Copilot answers without checking citations to understand where Copilot sourced the information from. • Saving Copilot-generated meeting notes as the official record without checking for accuracy.
For generating relevant images, i.e. to explain a concept or suit your presentation slides.	For personal or private details not required for the task. For example: • Health information, disciplinary issues, or HR complaints. • Private financial data. • Identifiable details about members of the public unless essential and permitted. Keep prompts to the *minimum necessary personal data* for the task.
When playing a role or persona, i.e. "an expert in writing easy to follow user guides" or "an analyst turning complex analysis into plain language".	With information that could breach an OIA, Privacy Act or other legal obligation. For example: • Draft OIA responses prior to clearance. • Names of staff being considered for redundancy, medical retirement, or performance processes. • Internal legal advice that is privileged. • Material sourced from agencies that has caveats like "Do not circulate". When in doubt, summarise the scenario rather than pasting the text.
For rewording a Kāinga or SharePoint page.	
For writing tasks, such as drafting emails and editing text for clarity, grammar and spelling.	
When answering specific search questions.	
For generating ideas, i.e. brainstorming ideas to get you started on a task.	
For technical assistance and troubleshooting.	

Released under the Official Information Act 1982

3. Protect classified information

CoPilot Chat is approved for use up to and including RESTRICTED DPMC held information.

4. Ensure human oversight for inputs and outputs

You remain accountable for your work. Always check and confirm the content for accuracy, including inputs, prompts and responses**.**

5. Respect mātauranga Māori

Mātauranga Māori is a living knowledge system and is based on the lived experience of whānau, hapū and iwi. AI tools, such as CoPilot Chat, are not well equipped to help with tīkanga or te reo Māori, and it is recommended you seek further guidance from those who are able to appropriately quality check the output generated.

6. Report all incidents and concerns

Report any misuse or potential security or privacy events involving CoPilot Chat to your manager.

APPENDIX 1: Related Policies and Guidance

Other documents and policies that should be read in conjunction with this guidance include:

- Generative Artificial Intelligence (Gen-AI) Policy (iManage 4971102)
- IT and Communications Technology Acceptable Use Policy (iManage 551779)
- The Joint System Lead's Generative AI Guidance for the Public Service
- AI and the Information Privacy Principles (Office of the Privacy Commissioner)
- Information and Records Management Policy (iManage 4795726)
- Privacy Policy (iManage 3082772)
- Procurement Policy (iManage 3871178)
- Protective Security Policy (iManage 4342432)
- Social Media Policy (iManage 4280517)

Released under the Official Information Act 1982