Defence House
34 Bowen Street
Wellington, New Zealand

P +64 (04) 496 0999
E info@defence.govt.nz

PO Box 12703
Molesworth Street
Wellington 6144, New Zealand

www.defence.govt.nz

MANATŪ KAUPAPA WAONGA
NEW ZEALAND
MINISTRY OF DEFENCE

31 October 2025

RESPONSE TO YOUR OFFICIAL INFORMATION ACT REQUEST

Thank you for your email of 16 October 2025, in which you requested, pursuant to the Official Information Act 1982 (the Act), responses to four questions regarding the Ministry of Defence's (the Ministry's) use of artificial intelligence.

The Ministry is a civilian agency that is responsible for the development of defence policy, international defence engagements, and the delivery of major capability projects. We are a separate agency from the New Zealand Defence Force (NZDF), which includes the military services.

Your questions are answered below.

> *To better understand the government's use of artificial intelligence (AI), I request the following information:*
>
> 1. *A list of all AI tools that are currently approved for use by staff at your agency.*

Microsoft Copilot Chat is approved for use by the Ministry's staff.

> 2. *Any documentation outlining the conditions, guidelines, or policies attached to the approval and use of these tools.*

The Ministry's use of AI is within the context of the *Responsible AI Guidance for the Public Service: GenAI* which provides overarching expectations regarding where the Public Service is working or planning to work with generative AI. These are available from https://digitial.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/responsible-ai-guidance-for-the-public-service-genai/overview.

The Ministry's corporate policy on the use of AI is enclosed. Work is being undertaken to update the policy to reflect the recent introduction of Copilot Chat.

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.*

   and

4. *Copies of all completed Cloud Risk Assessments and Privacy Impact Assessments (or equivalent documents) for each of the approved AI tools.*

The Ministry receives ICT services from the NZDF. This enables the Ministry to leverage economies of scale and supports collaboration including in the development of advice on Defence policy and deployments, and the delivery of military capability. Copilot Chat is part of the broader Microsoft 365 licence, which is managed by the NZDF.

Information relating to questions 3 and 4 is best addressed by the NZDF, who manage the broader Defence ICT environment that the Ministry receives as a service. As such, your request has been passed to the NZDF for response, and they will respond to you directly in due course. Given the Ministry does not hold this information itself, these elements of your request are declined pursuant to section 18(e), that the information requested does not exist or, despite best efforts to locate it, cannot be found.

Under section 28(3) of the Act you have the right to request the Ombudsman to investigate and review this response.

Yours sincerely

Hamish Rogers
Deputy Secretary, Governance People and Executive Services

Enclosed:

- *Ministry of Defence guidance: Expectations Regarding the use of Generative Artificial Intelligence*, April 2025

cc: NZDF Ministerial Services
ministerialservices@nzdf.mil.nz

MANATŪ KAUPAPA WAONGA
NEW ZEALAND MINISTRY OF DEFENCE

GUIDANCE: **EXPECTATIONS REGARDING THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE**

Policy Owner	Governance, People and Executive Services
Contact Person	Mel Childs, Deputy Secretary Governance, People and Executive Services
Approved By	Strategic Leadership Team
Approval Date	April 2025
Review Date	April 2027

Purpose

1. This document sets out the Ministry of Defence's expectations regarding the use of generative Artificial Intelligence (AI)[1] tools by Ministry employees. This guidance seeks to balance the opportunities and risks, along with the existing guardrails in place. This includes but is not limited to privacy, security, and ethical considerations.

Introduction

2. At present, generative AI tools can only be used on a trial basis using non-sensitive information and with the below controls.

3. Staff must not access generative AI tools using Defence credentials or on standard NZDF-managed devices, such as DIXS and Defence-provided iPads and iPhones. Dedicated, standalone devices are to be used for testing generativeAI tools.

4. Generative AI and other FuturesTech capabilities can offer significant benefits for government, particularly in efficiency, innovation, and service delivery.

5. **Defence has not yet undertaken reviews of these tools** – including for security and privacy considerations – and so sensitive information must not be input or uploaded to these tools at this time. However, there are opportunities to trial generative AI tools on public information in careful ways to build our understanding of the tools and the associated opportunities.

6. **Deputy Secretary oversight is required** where Ministry information is put into the generative AI tools and when drawing on information generated by AI tools for the purpose of Ministry work.

Definitions

7. Generative AI are tools that use large amounts of information (including personal information) to transform and generate a variety of content, including human-like conversations, writing essays, creating images or videos, and computer code.

[1] Refers to the capability of machines to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving and decision making.

8. Generative AI is an umbrella term for tools and applications which use large volumes of information to generate or transform a variety of text, audio, and visual media in response to prompts. Generative AI learn the patterns and structure of their inputs, including incorporating feedback on its accuracy, to generate new data with similar characteristics.

9. Prominent generative AI tools include: OpenAI's ChatGPT; Microsoft's Bing search or Copilot products, which leverages GPT-4; Google's Bard; and Midjourney.

10. Generative AI tools and their impacts are evolving rapidly, with regulators worldwide actively reviewing and implementing policy to address potential risks. There has been recent public concern around morality, plagiarism, impersonation and false representation of source documents regarding generative AI. AI systems may also not always comprehend real-world contexts, nuances in language, cultural references and intent and as a result have significant limitations.

11. Generative AI should be recognised as only a tool which can help focus on outcomes, but is not an end in of itself. Generative AI responses are helpful for stimulating thought and providing suggestions, but are typically limited in their ability to generate genuinely new and high quality critical content.

Principles and Policy

12. AI tools have not been reviewed and accredited to hold sensitive Ministry information, as is required for all Defence systems.

    12.1. Generative AI poses unique information management, privacy and cyber security issues. Defence requires robust testing of new technologies, including generative AI tools, to ensure they are fit for purpose when considering ethics, security, privacy, data quality, commercial relationships and legality. Until this has occurred, use of these tools must be limited to trials drawing on non-sensitive information.

    12.2. In accordance with existing policy no sensitive information is to be put into AI tools – including national security information (RESTRICTED or higher), SENSITIVE or IN CONFIDENCE. As a general rule, any information that would be withheld under the Official Information Act 1982 should not be input into AI tools.

13. Generative AI and other FuturesTech capabilities could offer significant benefits for government, particularly in efficiency, innovation, and service delivery. It is useful for the Ministry to build an understanding of these tools in careful and managed ways, but at this time this involves trialling using non-sensitive information.

14. Caution is needed when trialling generative AI tools:

    14.1. Deputy Secretary approval is required prior to inputting permitted Ministry information into generative AI tools, to ensure review and oversight of the sensitivities of the information being used.

    14.2. Ministry staff must not use Defence credentials (including Defence email addresses) to access external generative AI applications. It should be assumed that information submitted to AI tools is uncontrolled.

    14.3. Ministry staff must not access generative AI tools on standard NZDF-managed-devices – including DIXS, iPads and iPhones. Dedicated, standalone devices will made available for testing such tools.

    14.4. Ministry staff must not rely on the outputs of generative AI as being factually accurate without reasonable levels of validation and fact-checking and Deputy Secretary approval is required before drawing on AI tool-generated information for the purposes of Ministry work. Generative AI can be biased as a result of inputs, machine learning, and the nature of their development. The accuracy, reliability and sourcing of AI outputs often cannot be determined and can further perpetuate bias and discrimination.

14.5. Ministry staff must, where practical, ensure that content generated outside of the Ministry, but which is being used by the Ministry, adheres to the policies and principles of this guidance.

15. Where the Ministry holds information generated by AI tools, this must be clearly labelled, and its source must be made apparent when used as the basis for decision making, both within the Ministry and when engaging with others.

16. Robust testing is required for all new technologies used for Ministry work, to ensure they are fit for purpose when considering ethics, security, privacy, data quality, commercial relationships and legality. In terms of risks from the use of generative AI, initial key concerns relate to:

16.1. our transparency responsibilities where we draw on outputs from AI tools for Defence work

16.2. the lack of clarity in relation to the source information being used to generate results – including where there may be copyright and privacy issues

16.3. the need to question the accuracy and bias of information provided by AI tools

16.4. a lack of clarity about how information supplied is used by AI tools and who else would have access to information input.

17. Generative AI tools, capabilities, and their impact are rapidly evolving. The Ministry will continue to consider the opportunities, issues and risks that this technology provides.

Relevant legislation and policies

18. Defence work is undertaken using the ICT tools and systems that are approved for operation following a review identifying security and privacy risks. The framework for the approval of such systems is set in the Ministry's *Security Policy* and *Managing Personal Information Policy*. Defence has not accredited any GenAI tools to hold sensitive information – including information with a national security classification (RESTRICTED or higher) and IN CONFIDENCE or SENSITIVE information with commercial, privacy or Cabinet sensitivities. This policy aligns with NZDF's CISO Directive 01/2023 *Restrictions and Allowances on NZDF Use of Generative Artificial Intelligence*.

19. The Government Chief Digital Officer (GCDO) has issued its *Responsible AI Guidance for the Public Service: GenAI*, which supports leaders, decision-makers and those in the New Zealand Public Service working or planning to work with generative AI. It enables agencies to explore and adopt generative AI systems in ways that are safe, transparent and responsible and which effectively balance risks with potential benefits of these systems.

20. The GCDO's advice is part of the *Public Service AI Framework* that supports the responsible use of AI technologies across the public service. This defines five key principles:

Inclusive, sustainable development

20.1. 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

20.2. 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.

20.3. 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

20.4. 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.

20.5. To support this, agencies should publicly disclose:

20.5.1. when AI systems are used

20.5.2. how they were developed

20.5.3. how they affect outcomes — as relevant and appropriate according to the given use case.

20.6. Agencies should also enable people affected by the outcome of an AI system to understand how the outcome was determined.

Safety and security

20.7. 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.

20.8. 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

20.9. AI use within the Public Service should be subject to oversight by accountable humans with appropriate authority and capability at every stage.

20.10 This should include the application of relevant regulatory and governance frameworks, reporting, auditing and/or independent reviews.

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

21. In June 2024, Cabinet agreed to promote the *OECD AI Principles* as a key direction for New Zealand's approach to responsible AI. The OECD principles promote the use of AI that is innovative and trustworthy, and that respects human rights and democratic values.

22. The National Cyber Security Centre has issued joint guidance with partner country agencies regarding the secure use of AI:

22.1. *Guidelines for Secure AI System Development*, November 2023, is written to help AI developers to bake-in cyber security from the outset. It aims to help developers of any systems that use AI to make informed cyber security decisions at every early stage of the development process – whether those systems have been created from scratch or built on top of tools and services provided by others.

22.2. *Engaging with Artificial Intelligence*, January 2024, provides organisations with guidance on how to use AI systems securely. It summarises some important threats related to AI systems and prompts organisations to consider steps they can take to engage with AI while managing risk. It also provides mitigation to assist organisations that use self-hosted and third-party hosted AI systems, and is focused on using AI systems securely rather than developing secure AI systems.

22.3. *Deploying AI Systems Securely*, April 2024, outlines methodologies for protecting data and AI systems and responding to malicious activity. It aims to improve the confidentiality and integrity of AI systems and provide assurances that known vulnerabilities are mitigated.

23. In June 2024, the Office of the Privacy Commissioner issued expectations with respect to the use of generative AI by agencies. The Office expects that agencies considering implementing a generative AI tool will:

23.1. Have senior leadership approval

23.2. Review whether a generative AI tool is necessary and proportionate

23.3. Conduct a Privacy Impact Assessment

23.4. Be transparent

23.5. Engage with Māori

23.6. Develop procedures about accuracy and access by individuals

23.7. Ensuring human review prior to acting

23.8. Ensure that personal or confidential information is not retained or disclosed by the generative AI tool.

24. The Algorithm charter demonstrates a commitment to ensuring that New Zealanders have confidence in how government agencies use algorithms. The charter is one of many ways that government demonstrates transparency and accountability in the use of data.

Responsibilities

25. Ministry staff must obtain the agreement of their Deputy Secretary:

25.1. before putting Ministry information into an AI tool, in order to manage the sensitivities of the information being used, and

25.2. before drawing on AI tool-generated information for the purpose of Ministry work. This is to consider risks, including bias.

26. A request to a Deputy Secretary to trial an AI tool must include a use case and risk assessment. When assessing the use of a generative AI tool, the Deputy Secretary may seek advice from security, privacy, information management and ICT technical experts to ensure appropriate mitigations are in place.