Headquarters
New Zealand Defence Force
Defence House
Private Bag 39997
Wellington Mail Centre
Lower Hutt 5045
New Zealand

OIA-2026-5750

21st May 2026

[redacted]@pg.canterbury.ac.nz

Dear [redacted]

I refer to your email of 3 April 2026 requesting, under the Official Information Act 1982 (OIA):

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*
   - *Any internal documents specifying data residency or data sovereignty requirements in connection with your productivity platform*
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*
   - *Any security assessment, risk assessment, or privacy impact assessment produced in connection with the use of any cloud infrastructure provider*
   - *Any internal documents specifying data residency or data sovereignty requirements in connection with cloud infrastructure*
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*
   - *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*
   - *Any risk assessment, privacy impact assessment, or security assessment produced in connection with the adoption or use of AI tools at your agency*

The New Zealand Defence Force (NZDF) has contracts through the All of Government (AOG) procurement process with Microsoft 365 for E5 licences and Microsoft Azure Infrastructure as a Service Cloud. The Cabinet papers for the NZDF Enterprise Productivity Business Case

and Enterprise Cloud and Connectivity are publicly available on the NZDF website.[1] There is no agency order form. Because of the nature of NZDF information, documents concerning data sovereignty, security, and risk assessments are withheld in full in accordance with section 6(a) of the OIA. Enclosed is a copy of the privacy assessment for Microsoft Azure Cloud. Where indicated, sensitive security information is withheld in accordance with section 6(a) of the OIA.

The NZDF uses Copilot Chat as part of the Microsoft E5 licensing agreement. Copies of associated documentation are publicly available on the NZDF website.[2]

You have the right, under section 28(3) of the OIA, to ask an Ombudsman to review this response to your request. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that responses to official information requests are proactively released where possible. This response to your request will be published shortly on the NZDF website, with your personal information removed.

Yours sincerely

GA Motley
Brigadier
Chief of Staff HQNZDF

Enclosure:
1. Cloud infrastructure privacy assessment

[1] https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/New-Zealand-Defence-Force-Enterprise-Productivity-Business-Case-v4.pdf
https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/defence-force-enterprise-cloud-and-connectivity.pdf
[2] https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/OIA-2025-5581-AI-tools.pdf

PRIVACY ACT 2020 PRINCIPLES AND CONSIDERATIONS

1. The Privacy Act 2020 governs how organisations can collect, store, use and share information. It ensures that the organisation knows when information is collected, used and shared appropriately, and kept safe and secure. Data privacy is ensuring the legal rights of people whose data has been collected, has been respected. The following must be ensured:

   a. The people whose data has been collected know why is has been collected, how it will be used, and where the data goes.

   b. The data flows appropriately from the person to the organisation, inside the organisation (access to data is controlled), and outside the organisation. Disclosures must be carefully considered. This point is more specific to data sovereignty and discussed in the below table.

2. This paper considers the 13 Privacy Act principles and identified those principles that are relevant to the Defence Force's usage of Microsoft Azure Cloud s. 6(a) .

3. The risk area each of the identified privacy principles is linked to has also been noted, as these increase the overall impact of identified data sovereignty risks being realised.

Principle	Detail	Risk Linkage	Relevance data Sovereignty
Principle 1 - Purpose of collection of personal information	Organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose.	N/A	Not relevant because this principle relates to the collection of data.
Principle 2 - Source of personal information - collect it from the individual	Personal information should be collected directly from the person it is about.	N/A	Not relevant because this principle relates to the collection of data.
Principle 3 - Collection of information from subject - what to tell the individual	Organisations should be open about why they are collecting personal information and what they will do with it. This principle is about helping people understand the reasons you are collecting their information.	N/A	Not relevant because this principle relates to the collection of data.
Principle 4 - Manner of collection	Personal information must be collected in a way that is lawful and seen as fair and does not unreasonably intrude upon the personal affairs of the individual concerned. .	N/A	Not relevant because this principle relates to the collection of data.

Principle 5 - Storage and security of information	Organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, access, misuse or disclosure of personal information.	Unauthorised Access Legislative Access	Increases the impact if the Defence Force experiences an Unauthorised Access and/or Legislative Access breach and data breached contains personal information as this may put the Defence Force in breach of the Privacy Act.
Principle 6 - Access to personal information	Organisations must provide access to the personal information if the owner of that information asks for it. People have a right to ask for access to their own personal information.	Availability of Data	Data may become inaccessible if an offshore server limits access due to technological failure or loss of control. This impacts the right to obtain data and impacts privacy.
Principle 7 - Correction of personal information	The owner of information has the right to ask an organisation or business to correct information about them if they think it is wrong.	Availability of Data Privacy	Same as above, with additional loss of access to rectify incorrect information.
Principle 8 - Accuracy of personal information	Organisations must check before using or disclosing personal information that it is accurate, up to date, complete, relevant and not misleading.	N/A	Not relevant because this principle relates to the accuracy of personal information that is disclosed.
Principle 9 - Retention of personal information	Organisations should not keep personal information for longer than it is required for the purpose it may lawfully be used.	N/A	Not relevant – Principle relates to the Defence Force's data retention policy
Principle 10 - Limits on use of personal information	Organisations can generally only use personal information for the purpose it was collected, and there are limits using personal information for different purposes.	N/A	Not relevant – Principle relates to a specific party using information. This principle is not applicable to the Defence Force in the event a Data Sovereignty risk was realised resulting in information used by another party.
Principle 11 - Disclosure of personal information	Organisations may generally only disclose personal information to another agency or any other person if the agency believes, on reasonable grounds, that the disclosure of the information is for the purpose for which it was originally collected or obtained. Sometimes other reasons for disclosure are allowed, such as disclosure for a directly related purpose, or if the person in question gives their permission for the disclosure.	N/A	Not relevant – in the event another party accessed Defence Force information through legislative or unauthorised access, the Defence Force has not disclosed any information to another party.
Principle 12 - Disclosure outside New Zealand	Organisations may only disclose personal information to another organisation outside New Zealand if they check that the receiving organisation:	N/A	Not relevant – In the event data was obtained through legislation or unauthorised access the Privacy Act applies to the party who distributes information not the Defence Force.

	• is subject to the Privacy Act because they do business in New Zealand • will adequately protect the information • is subject to privacy laws that provide comparable safeguards to the Privacy Act If none of the above criteria apply, the organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.		It is also noted that Microsoft is subject to the privacy laws of New Zealand.
Principle 13 - Unique identifiers	Organisations can only assign unique identifiers to individuals when it is necessary for its functions.	N/A	Not relevant – Principle not effected by use of Microsoft Azure cloud