

3 November 2025

File Ref: OIA 50549



Tēnā koe 

Official Information Act request

Thank you for your information request dated 16 October 2025. Your request has been considered under the Official Information Act 1982 (**Act**). Your questions and our responses are as follows:

“Approved Artificial Intelligence Tools This is a request made under the Official Information Act 1982. 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”.

Te Puni Kōkiri has only authorised the use of Microsoft M365 Copilot in its Copilot Chat (Basic) functionality and the fully licensed Copilot for Microsoft 365 version. No other AI tools have been authorised for use by staff for work purposes.

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

Two documents have been identified as in scope of this part of your request and my decisions with regard to the release of the information are set out in the table attached as **Appendix A** (Documents two and three refer).

“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”.

Te Puni Kōkiri has funded a total of 25 licenses/subscriptions of Copilot for Microsoft 365.

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

One document has been identified as in scope of this part of your request (Document One listed in **Appendix A** refers).

I trust my response satisfies your request.

You have the right to seek an investigation and review by the Ombudsman of this response. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that Te Puni Kōkiri publishes some of its OIA responses on its website, after the response is sent to the requester. The responses published are those that are considered to have a high level of public interest. We will not publish your name, address or contact details.

If you wish to discuss any aspect of your request with us, including this decision, please feel free to contact us at uia@tpk.govt.nz.

Nāku noa, nā

A handwritten signature in blue ink, appearing to read 'Manaia King', with a stylized flourish at the end.

Manaia King
Hautū, Te Puni Rangatōpū | Deputy Secretary, Corporate

Appendix A: Documents - OIA request from [REDACTED] dated 16 October 2025

Item	Date	Document description	Decision
1.	21 February 2024	PIA Copilot – Bing Chat Enterprise, privacy impact assessment of Microsoft BCE (now Copilot) for Te Puni Kōkiri	Released in full
2.	28 February 2025	AI Principles, outlining the guiding principles for the ethical, fair, safe and secure use of artificial intelligence technology by Te Puni Kōkiri	Released in full
3.	28 February 2025	AI Policy, providing guidance on the safe and responsible use of artificial intelligence technology by kaimahi within Te Puni Kōkiri	Released in full

FORM A - PRIVACY IMPACT ASSESSMENT FORM

“Personal information” held by Te Puni Kōkiri must be protected and dealt with in accordance with the Privacy Act 2020. “Personal information” is defined in the Privacy Act as *“information about an identifiable individual”*. As well as identifiers such as a person’s name or email address, less obvious examples such as age or employment status fall within this definition if the way the information is recorded identifies the individual. To ensure that Personal Information in Te Puni Kōkiri is handled in accordance with the Privacy Act, could you please complete the following assessment for your area of work.

Microsoft Copilot
<i>Describe the project.</i> Te Puni Kōkiri has not authorised or endorsed the use of Generative AI or Large Language Models for official use. However, we are aware that some kaimahi are using Microsoft Copilot, formerly called Bing Chat Enterprise (BCE). This PIA is being done to ensure that appropriate processes/systems/understandings are in place to protect personal information when kaimahi are engaging with Copilot. <i>Name of person responsible for the project</i> Richard Foy, Manager Knowledge Systems is leading work in relation to Microsoft Copilot, Generative AI and Large Language Models
<i>What is the project aiming to achieve and how will it support TPK’s work?</i> Microsoft Copilot, formerly known as Bing Chat Enterprise, is an AI-powered chatbot designed for use in business organisations. Copilot (unlike the public Bing Chat that comes as default with the Microsoft Edge browser) has Commercial Data Protection. According to Microsoft: ▪ User and business data in Copilot is protected and will not leak outside the organization. ▪ Chat data is not saved, and Microsoft has no eyes-on access to it. ▪ Additionally, chat data is not used to train the underlying models. Copilot could be used by kaimahi to: ▪ Wordsmith a document. ▪ Suggest potential content for a report or document. ▪ Summarise a long document. ▪ Suggest research sources.

Will new personal information be collected or will the project use information we currently hold?

Kaimahi could potentially input personal information into Copilot as part of their query. Copilot could potentially source personal information from its own search database and provide this personal information in its response to kaimahi queries.

How long will the project be in place and personal information be required?

Copilot is being used in BAU. Kaimahi will be made aware of, and be expected to comply with, their privacy obligations (under TPK's Personal Information Policy and Processes) in relation to any personal information Copilot may provide in response to their queries.

COLLECTION STAGE		
Privacy Act Requirements	Questions	Answers
TPK can only collect personal information, for a purpose that is related to a lawful function of TPK <u>and</u> the personal information must be necessary for the purpose TPK wants to achieve.	What is the purpose for which the Personal Information being/likely to be collected using Copilot? Is this purpose a lawful function of TPK? What Personal Information is being/likely to be collected using Copilot? Is TPK aware of the data sources Copilot is trained on and how reliable these sources are for our purposes? What assurances do you have that Copilot will provide accurate and reliable Personal Information. What steps are being taken to minimise any risks to Personal Information associated with the use of Copilot and the risk of privacy breaches?	Kaimahi have been given interim guidance to not use large language model AI technology for work purposes until there is more understanding of the risks associated with AI. (https://intranet.te-wheke.int/en/guides-and-tools/technology/guidelines-for-using-chatgpt). This would include using Copilot to collect personal information. Additionally, kaimahi have been given guidance that they need to be wary of entering any personal information into Copilot. This guidance points to our Personal Information Policy. (https://intranet.te-wheke.int/en/whats-on/kotuitui/chatgpt-to-use-or-not-to-use-find-out). However, we have been unable to turn off the AI chat feature in Microsoft Edge browser and realise that kaimahi may use it if it is readily available to them in a work tool. For this reason, we recognise additional guidance will be required to be given.

		The most likely use of Copilot within Te Puni Kōkiri would be to aid in writing documents, such as: - wordsmithing - suggesting possible content - finding out more about a particular topic This use of Copilot is certainly within the lawful function of Te Puni Kōkiri. TPK does not know what training datasets are being used to train Copilot. That information is not publicly available. We will be instructing kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they will be required to complete a separate PIA for that purpose. We can not make any assurances that any information Copilot provides will be accurate or reliable. As with any research on the Internet, any information received must be double-checked and assessed for accuracy. We will update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
In general, personal Information needs to be collected directly from the individual concerned and	Does Copilot use publicly available information to respond to queries?	We do not know what datasets have been used to train Copilot in order for it to provide information.

the individual must be informed of the following (Disclosure and Consent Process): • That the information is being recorded; • How it is being recorded (electronic and/or hard copy); • The purpose it is being collected for; • Name and address of Agency collecting and the Agency that will hold the information. • Whether supplying the information is voluntary; • Consequences if request for information is declined; • Who will be able to access and use the information; • That the individual has the right to access and to ask to have the information corrected; and • The information will be destroyed once it is no longer needed. An exception to this rule is where the personal information is publicly available.	If the answer to the above is 'no' then kaimahi have to obtain Consent Form from Legal Services for the individual to sign before their personal information is shared with you.	We can assume that large portions of the datasets are publicly available information. Microsoft have indicated that any information used in prompts or queries within our Bing Chat Enterprise is not retained and not added to the training dataset used by Microsoft for its AI. Consequently any personal information contained in any queries will not be retained. https://learn.microsoft.com/en-us/copilot/privacy-and-protections. However, we will be instructing kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they will be required to complete a separate PIA for that purpose. We will update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
---	---	--

USE STAGE		
If TPK staff are using Copilot to collect personal information they must be made aware of the Personal Information Policy	What steps have been taken to ensure that kaimahi handling this personal information have been made aware of the Personal Information Policy requirements and the Collection Use processes?	Kaimahi should not be using Copilot to collect personal information. If they have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure

requirements and the Collection Processes above.		that appropriate steps are taken to protect personal information. Our interim guidelines will be updated to address the privacy aspect of using Copilot. We will also be placing notices on the Intranet and informing Managers directly of these matters as well.
TPK cannot repurpose personal information it holds for a new purpose unless it is a directly related purpose, authorised by laws or a specific exemption under the Privacy Act applies.	What steps have been taken to ensure that kaimahi handling this personal information have been made aware of the Personal Information Policy requirements and the Collection Use processes?	Kaimahi should not be using Copilot to collect personal information or repurpose any personal information that comes to them. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information. Our interim guidelines will be updated to address this privacy aspect of using Copilot. We will also place notices on the Intranet and inform Managers directly of these matters as well.
If a third party is collecting the information for TPK then TPK must take reasonable steps to ensure that they comply with the privacy Act too.	Does Copilot use publicly available information for collecting personal information when kaimahi send a request through. If the answer to the above is 'no' then what steps have been taken to: • Require Copilot to comply with the Privacy Act; and • require that Copilot confirm that it has Privacy Act compliant processes in place for the collection, use, storage, and disclosure of the information?	We do not know what datasets have been used to train Copilot in order for it to provide information. We can assume that large portions of the datasets are publicly available information. Microsoft have indicated that any information used in prompts or queries within our Bing Chat Enterprise is not retained and not added to the training dataset used by Microsoft for its AI. (https://learn.microsoft.com/en-us/copilot/privacy-and-protections).

		However, we would certainly advise kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information. We will also update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
The Act requires Personal Information to be collected directly from the person themselves unless TPK has reasonable grounds to believe that the individual has authorised someone else to disclose their personal information to TPK.	Does Copilot use publicly available information to respond to queries ? If the answer to the above is 'no' then what steps have been taken to ensure that the individual has authorised the disclosure of their information by someone else?	As previous question.

ACCESS AND STORAGE STAGE		
Privacy Act Requirements	Question	Answer
Personal Information is classified as " <i>In Confidence</i> " information under TPK's Classified Information Policy. So, the following steps must be taken in relation to the hard copy files and any databases on which personal information is held:	If Copilot provides Personal Information in response to kaimahi queries, where will the Personal Information be held? Who will have access to the Personal Information provided by Copilot in response to queries?	No information received via Copilot is retained within Copilot itself. It relies on kaimahi copying and pasting the information to another source such as a Word document. (https://learn.microsoft.com/en-us/copilot/privacy-and-protections).

- Electronic files must be protected against illicit internal use or intrusion by external parties in accordance with Te Puni Kōkiri's Records Management Policy, Records Management Guide and Electronic Communication Policy. - Paper documents must be stored in accordance with Te Puni Kōkiri's Records Management Policy and Records Management Guide. - A list of authorised users will be approved by the responsible manager.	How will the Personal Information provided by Copilot be secure against loss or misuse? Where Personal Information provided by Copilot is to be held in a register, database or central file, has a list of "Authorised Users" been approved by the responsible manager? Has access to the centralised file/database/register been restricted to those who "need to know"? What steps have been taken to ensure that kaimahi who provide or obtain Personal Information through Copilot are aware of these privacy requirements?	Kaimahi will need to handle any such document according to Te Puni Kōkiri's Security Classification Policy, just as they would for any other document. Kaimahi should not be using Copilot to collect personal information. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information. We will also update the interim guidance to kaimahi to take into account the availability of Copilot, place notices on the Intranet and inform Managers directly of these matters as well.
"Unique Identifiers" can be used to protect the names of individuals and remove the "privacy" implications. For example, recording information alongside a reference number as a unique identifier rather than a name might make the individual unidentifiable. Care should be taken about adopting a unique identifier unless it is necessary to carry out the purpose efficiently. An identifier assigned by another Agency *(such as an IRD number) should not be used. Using alternative references such as "the client" might make the individual unidentifiable.	Will unique identifiers be assigned to Personal Information obtained or shared with Copilot? Why is this being done and what is the "unique identifier" system that is being proposed?	No unique identifiers are required for the use of Copilot.

The Act requires that: • Personal Information be kept up to date and accurate; and • individuals be able to access and correct personal information TPK holds about them. So, processes need to be in place to allow access and changes to Personal Information.	What processes have been put in place to ensure that: a. Kaimahi are aware of the data sources that Copilot is trained on; b. Personal Information obtained through Copilot and held by TPK is accurate; c. Individuals can access their information provided by Copilot and request changes? and d. Only authorised changes are made to the information? What steps have been taken to ensure that kaimahi have been made aware of this requirement?	Copilot is not a place where kaimahi can “store” personal information or any information. It can only be queried, and information received, similar to searching on Google. There is no way in which information can be accessed and corrected, but misinformation can be reported to Microsoft. (https://www.microsoft.com/en-nz/concern/bing). As previously mentioned, we have no way of knowing what datasets have been used to train Copilot in order for it to provide information. We will be instructing kaimahi not to input personal information in their queries, nor to ask for personal information about individuals. If they ever have a valid use case to do so, they will be required to complete a separate PIA for that purpose. This will ensure that appropriate steps are taken to protect personal information.
---	--	--

USE STAGE		
Privacy Act Requirements	Question	Answer
If the Personal Information is to be used for another purpose (i.e. not the purpose for which it was collected) then the consent of the individual must be obtained: - the responsible manager must approve the individual being approached for the new purpose; and - this new consent must be in writing and signed by the individual.	What steps have been taken to ensure that the consent of the individual is obtained before Personal Information is used for another purpose? What steps have been taken to ensure that kaimahi have been made aware of this requirement?	Kaimahi should not be using Copilot to collect personal information or repurposing any personal information that comes to them. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. Our interim guidelines will be updated to address this privacy aspect of using Copilot.
If you are electronically transmitting any personal information, then you must: - Double check that the email address that you are sending the information to is correct; - Add the following statement to the bottom of your email: <i>“Te Puni Kōkiri is the originating government agency for this email. This email contains personal information which can only be used or disclosed in accordance with the Privacy Act. If you are the intended recipient, then note that this information is disclosed “In-Confidence” and cannot be used for any purpose other than that which Te Puni Kōkiri has disclosed it to you. <u>If you are not the intended recipient of this information, please delete the email from your records</u></i>	What steps have been taken to ensure that kaimahi been made aware of this requirement?	Kaimahi should not be using Copilot to collect personal information. If they ever have a valid use case to do so, they should be instructed to fill in a separate PIA for that purpose. Our interim guidelines will be updated to address this privacy aspect of using Copilot.

<u>and notify the sender by return email that you have received the information in error.”</u> a. If you are transmitting Personal Information in paper form, then you must: i. post the information in a single sealed envelope with “<i>Private - To Be Opened By Addressee Only</i>” clearly written on the front of the envelope; and ii. include a return address on the envelope in case delivery is unsuccessful. b. If you are disclosing personal information outside New Zealand, seek advice from Legal Services about the terms of TPK’s contract with the foreign person or entity. The Privacy Commissioner’s website has a model disclosure agreement clause builder. c. If there is no contract between TPK and the foreign person or entity, then you must be satisfied that comparable safeguards or authorisation by the person concerned still apply to disclosure to foreign persons or entitles. You will need to undertake careful checks to be satisfied that you can rely upon this ground. Seek advice from Legal Services before relying on comparable safeguards.		
---	--	--

DISPOSAL STAGE		
Privacy Act Requirements	Questions	Answer
Personal information needs to be destroyed once it is no longer required for the authorised purposes. Disposal will need to be done in compliance with TPK's Records Management Policy. You will need to consider: a. Do other laws requiring documents to be retained such as the Public Records Act 2005 apply? b. How long will the information be required for? c. What steps will need to be taken to initiate and complete the disposal process.	How long will the information be required for? What steps have been taken to ensure that Personal Information is destroyed once no longer necessary i.e.: a. Who will initiate the disposal process? b. Who will authorise the actual disposal and c. Who confirms the information has been destroyed?	<i>Under the Public Records Act, Te Puni Kōkiri has developed a Disposal Schedule that covers the disposal of personal information. Personal information collected under this project will be disposed of in accordance the Disposal Schedule.</i>

PIA completed by Signature: _____

Date: _____

Manager Approval:

Date: _____

Legal Clearance_____
Signature: _____

Solicitor, Legal Services / /

Approved / Not approved

Manaia King

Chief Privacy Officer

Signature: _____

/ /

RELEASED UNDER THE
OFFICIAL INFORMATION ACT



Artificial Intelligence (AI) Principles | Ngā Mātāpono Atamai Hangahanga (AI)

These are the guiding principles for our adoption and use of AI tools within Te Puni Kōkiri. They are rooted in ethics, fairness, safety and security and will serve as the guiding framework for all AI policies and procedures that we develop.

In our use of AI, we will:

Protect Māori data sovereignty

We will protect Māori data sovereignty, and the rights of iwi, hapū, whānau and Māori as articulated in Te Tiriti o Waitangi.

[Māori data sovereignty](#) refers to the rights of Māori people to control the collection, ownership, and application of their data. There are six key principles:

- 1. Rangatiratanga (Authority):** Māori have the right to exercise authority over their data and information.
- 2. Whakapapa (Relationships):** Data should be managed in a way that respects the relationships between people, places, and things.
- 3. Whanaungatanga (Kinship):** Data governance should foster and maintain Māori kinship ties and community connections.
- 4. Manaakitanga (Care and Respect):** Data should be used in ways that enhance the well-being of iwi, hapū, whānau and Māori communities.
- 5. Kaitiakitanga (Guardianship):** Iwi, hapū, whānau and Māori have a role as guardians of their data, ensuring it is protected and used responsibly.
- 6. Kotahitanga (Unity):** Data practices should promote unity and collective benefit for and with Māori.

These principles ensure that Māori data is managed in a way that aligns with Māori values and aspirations.

Ensure safety and security

We will use AI in ways that ensure the safety and security of our Ministry, our data, information and systems, our kaimahi and stakeholders, and the public.

Be ethical, just and fair

We will use AI in ways that promote fairness, abide by the laws of New Zealand, and do not unjustly harm, exclude, disempower or discriminate against individuals or particular groups.

In doing so we will:

Be transparent

We will be open about our use of AI and how we use it in our mahi.

Be accountable

We will take responsibility for our use of AI and any decisions we make.

Ensure accuracy and reliability

We will review AI output for accuracy, relevance and potential bias before using it.

Protect privacy

We will keep personal information of kaimahi, stakeholders and the public safe and secure when using AI.

Protect and govern data and information

We will properly manage and control access to our data and information when using AI. We will keep it safe from people viewing or sharing it without permission, whether on purpose or by accident. We will also keep safe any data or information that belongs to others when we use AI.

Commit to ongoing monitoring, learning and development

We will monitor our use of AI and continuously learn to improve. We will stay updated on developments in AI technology, practice, policy and guidelines, and incorporate new tools and practices where appropriate. We will continually learn how to make the best use of AI and incorporate it in our mahi.

Principles approval | Ko te whakaaetanga o te kaupapa

These principles owned and updated by:	They were approved by:	On the date of:	They are due for revision by:
Information Systems	The Deputy Secretary - Governance		

Acknowledgement [of the use of AI] | Te āhukahuka i [te whakamahinga o te AI]

Artificial Intelligence was used in the development of these principles. Specifically, AI tools were used to:

- Provide ideas and suggestions around potential principles to consider
- Create sentences around specific concepts
- Wordsmith and create a cohesive tone
- Suggest resources

Related documents | Ko ētahi atu kaupapa here

[AI Policy for Te Puni Kōkiri](#)

This policy sets out the acceptable use of AI tools within Te Puni Kōkiri.

[Information Management Policy](#)

The purpose of this policy is to provide a framework and assign responsibilities for ensuring that full and accurate records are created and managed.

[Information Security Policy](#)

This policy defines the principles, expectations, roles, and responsibilities to support Te Puni Kōkiri in upholding its Information Security responsibilities.

[Security Classification Policy](#)

This policy sets out the rules for protecting and handling information through the use of security classifications.

[Personal Information Policy](#)

The purpose of the Personal Information policy is to ensure effective processes are in place for all Personal Information held by Te Puni Kōkiri.

[Interim generative AI guidance for the public service. GCDO \(July 2023\)](#)

This guidance provides initial advice from the data, digital, privacy, procurement, and security System Leaders about Public Service use of generative AI tools. This guidance is intended to support agencies to make more informed decisions about using generative AI, balancing benefits and risks.

[Algorithm charter](#)

Algorithm Charter of Aotearoa New Zealand promotes the responsible and ethical use of algorithms in the public sector, ensuring that they are used in ways that are transparent, fair, and accountable. Te Puni Kōkiri is a signatory of this charter.

[AI Principles and Māori Data Sovereignty](#)

Tiriti-based AI Principles of Tino rangatiratanga, Equity, Active protection, Mana whakahaere, Mana motuhake, Tapu/noa.

[Te Mana Raraunga Māori Data Sovereignty](#)

This Te Mana Raraunga (TMR) Brief provides a general overview of key Māori Data Sovereignty terms and principles.

Contact | Whakapā mai

If you have any questions regarding this policy, you can contact the Manager, Knowledge Systems.



Why we have this policy | Ko te pūtake o tēnei kaupapa here

AI technology has grown exponentially in the last few years and is becoming increasingly integrated into our everyday tools. This policy provides guidance that allows us to use AI safely and responsibly at Te Puni Kōkiri. It enables us to take advantage of AI tools to enhance our mahi while also acknowledging and mitigating associated risks such as security and privacy breaches, bias, inaccuracy and lack of Māori data sovereignty.

This policy should be read in conjunction with our AI Principles, [the Interim Generative AI guidance for the public service](#), and [the Algorithm Charter for Aotearoa New Zealand](#).

In cases where issues are unclear, please consult the Manager, Knowledge Systems.

Policy | Kaupapa here

Te Puni Kōkiri provides you with access to approved AI tools to assist you in your mahi. This policy sets out acceptable use of AI in undertaking your mahi.

Use of AI tools | Te whakamahi i ngā taputapu AI

- You must only use AI tools that have been approved by Information Systems and have passed appropriate security and privacy assessments. Contact the [Helpdesk](#) for information on how to seek approval for an AI tool or system.
- While using AI tools, you must not (unless explicitly authorised):
 - input personal data or personal information, or query for personal information about an individual.
 - input any information or data that is classified IN-CONFIDENCE or above, as defined by the [Protective Security Requirements](#).
 - input any information that meets the criteria listed under sections 6 or 9 of the [Official Information Act 1994](#).
- You must check the accuracy of all AI output that is incorporated into your mahi and, where possible, cite reference sources.
- You must consider the sovereignty of any Māori data or information being used, either as input or output of AI and, where appropriate, seek permission for use.
- You must not breach intellectual property or copyright belonging to others in your use of AI. When inputting data or information into an AI tool, ensure you have the right to do so.
- You must consider the relevance and potential bias of any AI output that you incorporate into your mahi.
- You must acknowledge the use of AI tools if they have significantly contributed to a piece of mahi or a decision.
- You must take responsibility for any AI outputs you choose to include or incorporate in your mahi.
- You must take responsibility for any decisions you make, even if the decision has been influenced or recommended by AI.

- You must abide by the Te Tiriti based [Māori Data Sovereignty Principles/ Te Rangatiratanga o Rauranga](#) while using AI Tools:
 - Principle 1: Rangatiratanga (Authority) – You must recognise and uphold the right of iwi, hapū whānau and Māori to control their data, ensuring their authority is respected in all data-related activities.
 - Principle 2: Whakapapa (Relationships) – You must commit to manage data in a manner that respects and maintains the connections between people, places, and things, acknowledging the importance of whakapapa.
 - Principle 3: Whanaungatanga (Kinship) – You must take responsibility for the data governance practices to support and strengthen community and family ties, fostering a sense of kinship and belonging.
 - Principle 4: Manaakitanga (Care and Respect) – You must take responsibility to use data in ways that enhances the well-being of iwi, hapu, whānau and Māori communities, demonstrating care and respect in all data practices.
 - Principle 5: Kaitiakitanga (Guardianship) – You must acknowledge your role as a guardian of Māori data, ensuring it is protected and managed responsibly for the benefit of current and future generations.
 - Principle 6: Kotahitanga (Unity) – You must take responsibility that your data practices promote unity and collective benefit, working towards the shared goals and aspirations of iwi, hapū, whānau and Māori communities.

These policy statements ensure that our data practices align with Māori values and principles.

Consequences of breaching this policy | Ngā hua o te whati i tēnei kaupapahere

Any breach of this Policy may constitute misconduct and will be dealt with in accordance with the [Disciplinary Process Policy](#) of Te Puni Kōkiri.

Responsibility and enforcement | Ko ngā haepapa me ngā uruhi

This policy applies to all employees and authorised contractors of Te Puni Kōkiri.

Role	Responsibilities
All employees and authorised contractors	Are expected to comply with this Policy.
Deputy Secretary – Governance	The Deputy Secretary – Governance is the Chief Security Officer and is responsible for developing and implementing security procedures consistent with the Protective Security Requirements (PSR) and this policy.
General Manager – Information Systems	The General Manager – Information Systems is the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) and is responsible for developing and maintaining our information security programme and ensuring compliance with relevant policies and standards, consistent with the PSR.

Managers	Managers are responsible for ensuring their employees complete all relevant training and adhere to the policy.
----------	--

Monitoring and revision [of the policy] | Te aroturukitanga me te whakahounga [o te kaupapahere]

AI technology is changing rapidly. Opportunities, risks, and impacts of AI should be monitored and evaluated frequently, and changes made to this policy as needed.

Policy approval | Ko te whakaaetanga o te kaupapa

This policy is owned and updated by:	It was approved by:	On the date of:	It is due for revision by:
Information Systems	The Deputy Secretary – Governance		

Acknowledgement [of the use of AI] | Te āhukahuka i [te whakamahinga o te AI]

Artificial Intelligence was used in the development of this policy. Specifically, AI tools were used to:

- Create sentences around specific concepts
- Wordsmith and create a cohesive tone
- Suggest resources

Related documents | Ko ētahi atu kaupapa here

[AI Principles for Te Puni Kōkiri](#)

These principles set the guiding framework for any policies and processes developed within Te Puni Kōkiri for use of AI tools.

[Information Management Policy](#)

The purpose of this policy is to provide a framework and assign responsibilities for ensuring that full and accurate records are created and managed.

[Information Security Policy](#)

This policy defines the principles, expectations, roles, and responsibilities to support Te Puni Kōkiri in upholding its Information Security responsibilities.

[Security Classification Policy](#)

This policy sets out the rules for protecting and handling information through the use of security classifications.

[Personal Information Policy](#)

The purpose of the Personal Information policy is to ensure effective processes are in place for all Personal Information held by Te Puni Kōkiri.

[Interim generative AI guidance for the public service. GCDO \(July 2023\)](#)

This guidance provides initial advice from the data, digital, privacy, procurement, and security System Leaders about Public Service use of generative AI tools. This guidance is intended to support agencies to make more informed decisions about using generative AI, balancing benefits and risks.

[Algorithm charter for Aotearoa New Zealand](#)

The Algorithm Charter for Aotearoa New Zealand promotes the responsible and ethical use of algorithms in the public sector, ensuring that they are used in ways that are transparent, fair, and accountable. Te Puni Kōkiri is a signatory of this charter.

AI Principles and Māori Data Sovereignty

Tiriti-based AI Principles of Tino rangatiratanga, Equity, Active protection, Mana whakahaere, Mana motuhake, Tapu/noa.

[Te Mana Raraunga Māori Data Sovereignty](#)

This Te Mana Raraunga (TMR) Brief provides a general overview of key Māori Data Sovereignty terms and principles.

Glossary of terms | Te rārangi kupu

AI (Artificial intelligence)

Artificial intelligence (AI) is a field of computer science and machine learning that allows computer systems to perform tasks that typically require human intelligence. These tasks can include things like learning from data, recognizing patterns, making decisions and solving problems. AI enables computers to think, learn, and act in ways that mimic human intelligence, allowing them to tackle complex tasks and adapt to new situations without explicit programming.

GenAI (Generative AI)

Generative AI (GenAI) is a type of AI that uses prompts to generate responses that closely resemble human-created content. This content can be in the form of text, images, video, or audio.

Input

Input refers to any text, image, audio, video, code, link, data, dataset, or document provided as a prompt to an AI tool.

Māori Data

Is defined as the “Digital or digitisable information or knowledge that is about or from Māori people, language, culture, resources, or environments”. Māori Data is a Taonga and subject to Māori Governance.

Māori Data Sovereignty

Is “Māori Data Governance. The principles, structures, accountability mechanisms, legal instruments, and policies through which Māori exercise control over Māori data”.

Māori Data Sovereignty Principles/ Te Rangatiratanga o Rauranga

Is a modified set based on the academic position of Te Mana Raraunga to embed more traditional tikanga and Te ao Māori perspectives and individual, whānau, hapū, marae, rōpū and Iwi Sovereignty is recognised as outlined in Te Tiriti o Waitangi.

Output

Output in Generative AI refers to any text, image, audio, video, code, or document generated by an AI tool.

Contact | Whakapā mai

If you have any questions regarding this policy, you can contact the Manager, Knowledge Systems.