Te Kawa Mataaho
Public Service Commission

5 November 2025

9(2)(a) privacy

9(2)(a) privacy

Official Information Request
Our Ref: OIA 2025-0123

I refer to your Official Information Act 1982 (OIA) request received on 16 October 2025:

> *"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.*
> 2 *Any documentation outlining the conditions, guidelines, or policies attached to the approval and use of these tools.*
> 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.*
> 4 *Copies of all completed Cloud Risk Assessments and Privacy Impact Assessments (or equivalent documents) for each of the approved AI tools."*

Information being released

Listed below are the Artificial Intelligence (AI) tools Te Kawa Mataaho Public Service Commission (the Commission) has approved for use by staff. The Commission has five paid preliminary licences for Microsoft Copilot.

Corporate AI tools: Microsoft Copilot Chat and Microsoft Copilot

Generative AI (GenAI) tools: ChatGPT/OpenAI, Canva and Gemini.

Staff must never input official, classified, personal, or sensitive information into public GenAI tools, nor include organisation-specific details in prompts. These tools are suitable only for general queries or creative tasks that do not involve protected data.

Please find enclosed and listed in the table below the following documents in scope of part two of your request:

Item	Date	Document Description	Decision
1	September 2025	Artificial Intelligence Policy	Released in full
2	September 2025	Artificial Intelligence Guidance	Released in full
3	September 2025	Information Security - Acceptable Use Policy	Released in full

Information being withheld

There is a document covered by part four of your request that I have decided to withhold in full under section 9(2)(k) of the OIA to prevent the disclosure or use of official information for improper gain or advantage.

The document I am withholding either contains (or could be used to infer) important details about the Commission's security controls and/or any vulnerabilities we may have. This information could then be used to target our information systems.

In making my decision, I have considered the public interest considerations in section 9(1) of the OIA.

If you wish to discuss this decision with us, please feel free to contact Enquiries@publicservice.govt.nz.

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

Please note that we intend to publish this letter (with your personal details removed) and enclosed documents on the Commission's website.

Yours sincerely

Nicky Dirks
Manager – Ministerial and Executive Services
Te Kawa Mataaho Public Service Commission

INTERNAL POLICY

Te Kawa Mataaho
Public Service Commission

Artificial Intelligence Policy

Version	1.0	**Contact**	Chief Information Officer
Policy Owner	Deputy Chief Executive, Enabling Services	**Approved**	September 2025
SharePoint	The Hub, AI Hub	**Due for Revision**	July 2026

Context

AI technology has grown exponentially in the last few years and is becoming increasingly integrated into our everyday tools. This policy provides guidance to use Artificial Intelligence (**AI**) safely and responsibly at Te Kawa Mataaho Public Service Commission (the Commission). It enables us to take advantage of AI tools to enhance our mahi while acknowledging and mitigating associated risks such as security and privacy breaches, bias, inaccuracy and lack of Māori data sovereignty.

This policy outlines what is considered acceptable use of AI to conduct the Commission's business.

This policy is in addition to the Commission's **Information Security Acceptable Use Policy**.

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

Scope

This policy applies to all Commission kaimahi (including employees and secondees) and contractors that use the Commission's information systems.

Key definitions

There are several terms that are used in the policy which have a specific meaning:

- **Corporate AI tools** - These are AI tools that are formally approved and integrated into the Commission's systems and workflows. Examples include Microsoft Copilot, SharePoint-integrated AI, and other enterprise-grade AI services. These tools are subject to internal governance, security controls, and data handling protocols, and are considered safe for use with Commission information, including personal and restricted data.
- **Public Gen AI** – These are AI platforms available to the general public, typically hosted and managed by external providers, for example ChatGPT, Gemini, Canva etc. These tools are not managed by the Commission and store or process data externally.
- **Must**: adherence with the policy statement is mandatory.
- **Must not**: the action or behaviour described in the policy statement is prohibited.

Failing to adhere to this policy will be considered a policy/security breach and may result in disciplinary action.

Policy

The Commission is committed to using AI responsibly, lawfully, and ethically in line with the principles outlined below. AI will only be used in line with our principles, through approved tools and always under meaningful human oversight, with all final decisions made by people, not machines.

This policy will evolve as AI technologies, practices, and public expectations change, supported by ongoing monitoring, learning, and development to keep pace with best practice.

Principles

The continual evolution of AI and the public's expectations of the public sector means that this policy will evolve over time. It is not exhaustive of all future opportunities and challenges posed by AI. For example, the Crown may have Treaty of Waitangi obligations arising from the development and use of AI in New Zealand. As this area develops, we will keep current with best practice and our obligations.

A set of policy principles have been established to articulate how we will use AI responsibly at the Commission. These principles also underpin the statements in this policy:

1. **Use Only Approved AI Tools** – We will only use AI tools that have been formally approved for use by the Commission. This ensures that all AI usage complies with our security, privacy, ethical, and operational standards. Using unapproved tools may introduce risks to our data, systems, and people. We will follow internal guidance on which tools are permitted and how they should be used.

2. **Accountability -** We remain fully accountable for our mahi. AI is a tool to support people, not to replace human judgement, critical thinking or decision-making. We ensure meaningful human oversight and control at the right stages of any AI-enabled process. We take responsibility for our use of AI and any decisions we make. All decisions made at the Commission will be human-made, and not AI-made decisions. This policy MUST be formally accepted by all individuals in scope of the policy and a record kept of the individual's acceptance.

3. **Trustworthy -** We will review AI output for accuracy, completeness and relevance. It is imperative to use verified sources and trustworthy information so we can confidently explain and stand behind the choices we make.

4. **Responsible data stewards** We will use AI in ways that ensure the safety and security of the Commission, our data, information and systems, our kaimahi and stakeholders, and the public. We will properly manage and control access to our data and information when using AI. However, if you do come across information you shouldn't have access to, you MUST escalate this to the Chief Information Officer for resolution.

5. **Ethical, Just and Fair Use** - We use AI tools lawfully, ethically and check for introduced bias. 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. This includes rights and interest of Māori under the Treaty of Waitangi. AI use will be subject to monitoring and oversight by the Commission and its IT providers.

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

7. **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.

Use of Commission approved Corporate AI

You must only use the approved AI tools for Commission mahi. The Commission will maintain a curated list of AI tools that have been assessed and approved for safe use. This list will be published and regularly updated in the AI Guidance document.

Data protection applies when using Corporate AI tools. This means these tools can be safely used with the Commission data and documents, and data does not inform the AI model (large language model), i.e. our data does not leave our environment and go into the public domain. All information security measures and monitoring that apply to our overall digital environment (M365), apply to corporate AI tools that will be rolled out in Tranche 1 (Microsoft Copilot suite of products). Your prompts and use of Commission approved Corporate AI is subject to monitoring and reporting. Therefore:

- You **CAN** enter or upload any official Commission information and documents into approved corporate AI tools.

The Commission kaimahi are encouraged to use these approved tools as their first option. If the available Commission approved tools do not meet the specific requirements of a task, kaimahi may then use approved public generative AI (GenAI) tools, in accordance with AI guidelines.

Use of Commission approved Public GenAI

Wherever possible, kaimahi must use approved Corporate AI tools for their mahi. Only AI tools that have been formally approved for use by the Commission may be used for official mahi purposes. The list of approved tools will be maintained in the AI Guidance.

Public Generative AI (GenAI) platforms do **not** provide data protection guarantees. Any information entered into these tools, including prompts and uploaded documents may be used to train their models and could become publicly accessible. Therefore, when using Public GenAI:

- You **MUST NOT** enter or upload any official, classified, personal, or otherwise sensitive information that is not intended for public release.
- You **MUST NOT** include any organisation-specific details in prompts. Refer to the AI Guidance for examples and further information.

Examples of Public GenAI tools include Google Gemini, OpenAI ChatGPT, and Canva GenAI.

The Commission will not actively block access to Public GenAI platforms unless they pose an unacceptable level of risk. Non-approved public GenAI tools can be used for personal use. However, these tools must **not** be used for Commission mahi unless they are explicitly approved and listed in the AI Guidance.

We recognise the evolving needs of our kaimahi and will consider requests for additional GenAI tools. Any new tool will undergo the standard software introduction process, including privacy, data, and security assessments, and require approval from the Investment Committee.

Responsibility and enforcement

Role	Responsibilities
Deputy Chief Executive – Enabling Services	Deputy Chief Executive – Enabling Services is the Chief Security Officer and is responsible for developing and implementing security procedures consistent with the Protective Security Requirements (PSR) and this policy.
Manager, Digital Services | Chief Information Officer And Chief Information Security Officer	Manager, Digital Services (Chief Information Officer (CIO)) and Chief Information Security Officer (CISO) are responsible for developing and maintaining our information security programme and ensuring compliance with relevant policies and standards, consistent with the PSR.
Manager, Digital Services | Chief Information Officer	Manager, Digital Services (Chief Information Officer (CIO)) is responsible for monitoring AI use for the purposes of tracking adoption as well as other inappropriate uses, such as attempted jailbreaks.
Managers	Managers are responsible for ensuring their employees complete all relevant training and adhere to the policy.
All employees and authorised contractors	Are expected to comply with this Policy.

Glossary of Terms

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, recognising 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.

Corporate AI tools - These are AI tools that are formally approved and integrated into the Commission's systems and workflows. Examples include Microsoft Copilot, SharePoint-integrated AI, and other enterprise-grade AI services. These tools are subject to internal governance, security controls, and data handling protocols, and are considered safe for use with Commission information, including personal and restricted data.

Public Gen AI – These are AI platforms available to the general public, typically hosted and managed by external providers, for example ChatGPT, Gemini, Canva etc. These tools are not managed by the Commission and store or process data externally.

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

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

Internal Guidance

Te Kawa Mataaho
Public Service Commission

AI Guidance

This document provides guidance and information regarding the use of AI at Te Kawa Mataaho Public Service Commission (the Commission). This document will be updated when required, to remain accurate. This document accompanies the Artificial Intelligence (AI) Policy as additional guidance.

The Commission is committed to the safe, transparent, and responsible use of artificial intelligence that enhances delivery, protects privacy and data integrity, upholds Te Tiriti o Waitangi, and supports innovation, fairness, and continuous improvement.

We publish our internal guidance and information so that we are as transparent as possible with our people regarding the intended use of AI at the Commission. Our approach to AI is aligned with GCDO AI Guidance.

What you CAN do with AI

- Treat AI as a draft generator, not a final authority
- Refine prompts and iterate to improve the results
- Use AI to brainstorm, summarise or reformat content
- Use only approved AI solutions*
- Use Commission data and information in corporate AI tools*

What you CAN'T do with AI

- Use Commission data and information in any Public Gen-AI tools*
- Rely on AI to make decisions
- Assume AI outputs are correct or complete
- Attempt to jailbreak or bypass system restrictions

*List of Approved AI Tools, both corporate and Public GenAI, is listed further in the document

Guidance for our AI Principles

Use of Only Approved tools

To ensure the safe, secure, and responsible use of AI, all kaimahi must use only AI tools that have been formally approved by the Commission. Using only approved tools ensures that all AI usage aligns with our security, privacy, ethical, and operational standards. It protects our people, data, and systems from unintended exposure or misuse, and supports our commitment to transparency, trust, and responsible innovation.

Do

- Only use approved AI tools, and in accordance with Guidance
- Use corporate AI tools (e.g. Microsoft Copilot Chat) for tasks involving Commission data, including personal, Restricted, or Sensitive information. These tools operate within our secure Microsoft 365 environment and are protected by our organisational security, privacy, and compliance controls.

- Use public generative AI tools (e.g. ChatGPT, Gemini, Canva GenAI) only for general queries or creative tasks that do not involve any Commission-specific, personal, or sensitive information.
- Check for the green shield with a tick (🛡) in Copilot Chat to confirm you are logged in via your Commission account and operating within the protected environment.

Don't

- Do not use unapproved AI tools for any Commission-related mahi.
- Do not input official, classified, personal, or sensitive information into public GenAI tools. These platforms may store, reuse, or train on your data, and cannot guarantee confidentiality or compliance with our standards.
- Do not attempt to bypass system restrictions or use AI tools outside of approved channels.

Accountability

We remain fully accountable for our mahi. AI is a tool to support people, not to replace human judgement, critical thinking or decision-making. We ensure meaningful human oversight and control at the right stages of any AI-enabled process. We take responsibility for our use of AI and any decisions we make.

While we use AI to assist us with tasks, we are accountable for our decisions. We apply a risk-based approach to the use cases and the level of reliance we may choose to place on AI generated outputs.

Do

- Use AI to assist with tasks, not to make final decisions.
- Review all outputs before using them.
- Apply human oversight to all AI-assisted processes.
- Take ownership of final outputs and any decisions you make, even if it has been influenced or recommended by AI.
- Understand and verify outputs: AI can produce hallucinations - confident but incorrect responses - so human validation is necessary. Users must check AI outputs for accuracy, legality, bias, and cultural appropriateness.

Don't

- Delegate responsibility to AI.
- Use AI to make decisions without reviewing.

Trustworthy

We will review AI output for accuracy, completeness and relevance. It is imperative to use verified sources and trustworthy information so we can confidently explain and stand behind the choices we make.

Do

- Verify AI-generated content for accuracy, and where possible, cite reference sources.
- Use trusted sources to validate facts.
- Cross-check AI outputs.
- Use AI to explore options, not to confirm facts.

Don't

- Assume AI is always correct.
- Use unverified content in official work.

Responsible Data Stewards

We maintain the privacy of individuals and security of Commission/government information when using AI.

Do

- Monitor for misuse or unintended consequences.
- Escalate concerns about outputs with information you shouldn't have access to
- Follow security protocols.
- Follow privacy and data handling policies when handling both inputs in and outputs into AI.
- Report any data concerns.
- Apply access controls and audit trails.
- Respect data ownership and licensing.
- Follow classification and retention policies.
- Use secure platforms for storing AI-related data.
- Govern data according to internal policies.

Don't

- Share sensitive outputs via unsecured channels.
- Use third-party tools without approval.
- Input Commission data that is not publicly available into public generative AI.
- Store sensitive outputs in unsecured locations.

Ethical, Just and Fair Use

We use AI tools lawfully, ethically and check for introduced bias. 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. GenAI can perpetuate bias and outputs may reflect harmful stereotypes or inequalities, especially affecting Māori, Pacific Peoples, disabled people, and other communities.

Do

- Assess outputs for bias, fairness and inclusivity.
- Avoid reinforcing stereotypes or discriminatory patterns.
- Escalate ethical concerns.
- Test prompts for bias.
- Seek diverse input when designing AI use cases.
- When output is not right, either refine the prompt or the output itself.
- Use inclusive prompts.
- Validate outputs regularly.

Don't

- Use AI to make decisions that could unfairly impact people.
- Ignore flagged ethical issues or suspicious AI outputs.
- Use AI as a proxy for a consultation or cultural advice.
- Use AI for formal translation of Te Reo Māori.
- Use AI as a proxy for any consultation with Māori, or cultural advice or formal translation from Māori

Transparency

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

Do

- Be ready to explain your process.
- Share your approach when asked.
- Use inclusive prompts.

Don't

- Hide AI involvement.

Commitment 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.

Do

- Participate in training and capability sessions.
- Stay informed about new tools and risks.
- Provide feedback to improve AI use.
- Join AI communities of practice.
- Attend learning sessions.
- Advise our Digital Services team where you have a need for an AI tool that isn't met by the current approved solutions.

Don't

- Assume current knowledge is sufficient.
- Ignore updates to policy or guidance.

Corporate AI Tools

Corporate AI Tools Guidance

We encourage all kaimahi to actively explore and use approved corporate AI tools as part of their everyday mahi. These tools are designed to support, not replace, human intelligence, and their thoughtful use can significantly increase our capacity for meaningful engagement, critical thinking, and timely action. The more we use AI to streamline routine tasks, the more space we create for deeper collaboration, innovation, and human connection. By building confidence and capability in AI, we empower ourselves to work smarter, respond faster, and focus on what matters most.

Approved Corporate AI Tools

The following section describes the corporate AI tools that have been approved for use at the Commission.

1. Microsoft Copilot Chat

Copilot Chat is a Microsoft enterprise AI tool that provides secure, conversational assistance to employees. It leverages organisational data and Microsoft services to help users find information, automate tasks, and make informed decisions, all through natural language interaction.

Copilot Chat must only be used when logged in via your Commission account. This can be verified by confirming the green shield with a tick is showing in the Copilot Chat App.

When using Microsoft Copilot Chat through your Commission corporate account, enterprise protection ensures that all prompts, inputs, and outputs remain securely within our Microsoft 365 environment. This means your data is not used to train public AI models, is not accessible to external parties, and is protected by our organisational security, privacy, and compliance controls. You can safely use Copilot Chat to interact with internal documents, automate tasks, and generate content, knowing that your information is governed by the same protections as the rest of our digital ecosystem.

More information can be found here: https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection

Copilot Chat has no access to any of your, or the Commission's information. You can use general AI prompting, or you can upload a document for AI to reason over. Some of the uses for Microsoft Copilot Chat are:

- Asking a general question or advice about public information
- Using Commission information that has not been released to the public
- Drafting internal communications
- Uploading internal documents
- Generating generic images
- Generating images based on existing materials
- Analysing internal data

Public GenAI Tools

Public Gen AI Tools Guidance

Kaimahi are strongly encouraged to use Commission approved corporate AI tools as their first and primary option when incorporating AI into their mahi. These tools are designed to operate within our secure Microsoft 365 environment, offering enterprise-grade protection for all inputs and outputs. By using corporate AI tools, kaimahi can confidently engage with internal documents, automate tasks, and generate content, knowing that their data remains private, secure, and compliant with organisational standards.

Where corporate tools do not meet the specific needs of a task, kaimahi may use approved public generative AI (GenAI) tools, but only with caution and in strict alignment with our AI guidance. Public GenAI platforms, such as ChatGPT, Google Gemini, and Canva GenAI do not offer enterprise protection. Any information entered into these tools, including prompts, uploaded documents, or generated outputs, can be expected to be stored, reused, or used to train their models, and could become publicly accessible. Therefore, kaimahi must never input official, classified, personal, or sensitive information into public GenAI tools, nor include organisation-specific details in prompts. These tools are suitable only for general queries or creative tasks that do not involve protected data.

For example, a prompt such as *"I am working on a paper that is looking onto reducing public service by 10% by 2028. Can you give, in a table format, the number of kaimahi employed in NZ Public Service for each year from 2015 to 2025, by public service agency"*. This prompt would not be acceptable to be put into a public GenAI tool as it provides information regarding the (hypothetical) intent of reducing the public service by 10% by 2028, which would be considered Commission information. Instead, a prompt such as *"Can you give, in a table format, the number of kaimahi employed in NZ Public Service for each year from 2015 to 2025,* *by public service agency"* as it is a generic prompt and asking GenAI to reason over publicly available information.

Similarly, uploading a Commission document, that is not publicly available, is not an acceptable use of Public GenAI tools. Only publicly available documents and information can be uploaded to such tools. Where you require AI to reason over a Commission document or information, you need to use Commission approved AI tools.

Public GenAI tools are best suited for tasks like content creation, brainstorming, or answering general knowledge questions, but they should not be used for handling confidential or internal business data due to limited security and compliance controls. This is covered more in the sections below.

Approved Public GenAI Tools

The following section describes the corporate AI tools that have been approved for use at the Commission.

1. *ChatGPT*

A conversational AI tool developed by OpenAI that can generate text, answer questions, and assist with writing tasks. ChatGPT is hosted externally and may store or reuse input data. It should only be used for general queries or creative drafting that does not involve Commission-specific or sensitive information.

2. *OpenAI*

The company behind ChatGPT and other AI models such as GPT-4 and DALL·E. OpenAI provides APIs and web-based tools for generating text, images, and code. These services are public-facing and not covered by the Commission security protocols. Use only for non-sensitive, exploratory tasks.

3. *Canva*

Canva's AI-powered design tools include features like Magic Write and Magic Design, which generate text and visual content. These tools are useful for creative ideation and layout but are not approved for handling Commission-specific or sensitive data. Use only for general design tasks.

4. *Gemini*

Google's generative AI tool that can answer questions, summarise content, and assist with writing. Gemini is publicly available and may process data externally. It should not be used for Commission-related mahi involving sensitive or restricted information.

Corporate AI vs Public GenAI

The following table illustrates the type of information that can be used in Corporate AI tools vs Public GenAI tools

Type	AI Product	Prompts with Commission information	Commission data and documents	Generic prompts	Publicly available information and documents
Corporate AI	Microsoft Copilot Chat	✓	✓	✓	✓
	Microsoft Copilot (paid license)	✓	✓	✓	✓
Public Gen AI	ChatGPT	✗	✗	✓	✓
	OpenAI	✗	✗	✓	✓
	Canva	✗	✗	✓	✓
	Gemini	✗	✗	✓	✓

Examples of AI Use

TASK	PROMPT EXAMPLE(S)	COMMISSION APPROVED SOLUTIONS	PUBLIC AI (non-approved solutions)
Asking a general question or advice about public information	• *Write me a paper about artificial intelligence and it's use by university age students.* • *Explain the difference between a state-owned enterprise and a crown entity in New Zealand.* • *Summarise the GCDO guidance on AI usage in Public service from this website [user provides link].*	✓	✓
Using Commission information that has not been released to the public	• *Rewrite this policy on agency investigations in the New Zealand Public Service [user inserts copied text].* • *Analyse this data and report the findings [user uploads unreleased excel file].*	✓	✗
Drafting internal communications	• *Draft an email to all kaimahi about the new policy changes [copied text from internal policy].*	✓	✗
Uploading internal documents	• *Read these documents about internal policies and solidify them into one.*	✓	✗
Generating generic images	• *Create an image of people collaborating in the Public Service in New Zealand.*	✓	✓
Generating images based on existing materials (e.g. pictures of an event we have held or our logo that may be copyrighted or not have rights to use)	• *Create me a new word template with our logo image as inspiration [user uploads image].*	✓	✗
Analysing internal data	• *Analyse this dataset of employee performance metrics and provide insights.*	✓	✗

INTERNAL POLICY

Te Kawa Mataaho
Public Service Commission

Information Security – Acceptable Use Policy

Version	3.1	**Contact**	Chief Information Security Officer
Policy Owner	Deputy Chief Executive, Enabling Services	**Approved**	September 2025
SharePoint	Information Technology - Policies	**Due for Revision**	December 2025

This policy outlines what is considered acceptable use of Te Kawa Mataaho Public Service Commission (the Commission) information and technology systems to conduct Commission business.

What is acceptable use?

The aim of information security is to protect the confidentiality, integrity, and availability of information – in physical or electronic form – created, managed, or distributed by the Commission. Acceptable use is the personal responsibility of all Commission kaimahi and contractors in upholding this objective. This includes protecting systems that store and process information (such as laptops, mobile devices, and cloud services), as well as safeguarding physical information.

Principles

This policy addresses a variety of common acceptable use scenarios that the Commission will face. However, the continual evolution of technology and the public's expectations of the public sector means that this policy cannot provide guidance on every possible information security issue.

Therefore, a set of four policy principles have been established to articulate how we will achieve our desired information security posture. These principles also underpin the statements in this policy:

- Our people understand how to respond to the information security threats they are likely to encounter in their mahi.
- Our people are aware that they represent the Commission in everything that they do when using Commission information and technology systems.
- We use pragmatism and common sense when using information and technology and we seek advice when something doesn't seem right.
- We model how the public service can use information and technology effectively and securely.

When novel information security issues inevitably arise in the future, these principles will provide guidelines for framing a response that is aligned with the Commission vision and desired information security posture.

Scope and fit

This policy applies to:

- All Commission kaimahi (including employees and secondees) and contractors that use The Commission information systems.
- All third-party organisations that provide digital services to the Commission.

Key definitions

There are several terms that are used in the policy which have a specific meaning:

- **Must**: adherence with the policy statement is mandatory.
- **Must not**: the action or behaviour described in the policy statement is prohibited.
- **Should**: adherence with the policy statement is recommended but not required.
- **Should not**: the action or behaviour described in the policy statement should not be performed.

Failing to adhere to a Must or Must not statement will be considered a security breach and may result in disciplinary action.

Policy Acceptance

This policy MUST be formally accepted by all individuals in scope of the policy prior to them being granted access to the Commission systems and a record kept of the individual's acceptance.

- For new starters this MUST be done as part of their onboarding and induction process.
- For existing kaimahi, formal acceptance of the policy MUST be performed every two years or each time the policy is refreshed.

Policy

The following sections outline what is considered acceptable use of Commission information and systems to conduct Commission business. All unacceptable use will be investigated and addressed by Te Kawa Mataaho management and could result in disciplinary action.

Electronic communications

All communications relating to the Commission business MUST be sent and received using communications tools approved by the Commission. This includes your Commission email account and collaboration tools (such as Microsoft Teams and Zoom). Remember that you represent the Commission in all communications from your account.

Email

- All communications MUST be checked by the sender before sending to ensure these are addressed to the correct recipients and contain the correct information.
- Important emails containing information which is 'sensitive in nature[1]' SHOULD be checked by two people prior to sending. The Commission has developed guidance for this, the RECAP protocol (contained in Appendix A of this policy).
- The New Zealand Government's Protective Security Requirements Guidance (PSR) MUST be followed for the classification of information including attachments or content of emails. This guidance may require you to confirm the identities of recipients or encrypt attachments using approved software.

[1] Discretion should be used when deciding whether information is 'sensitive in nature'. This could include information classified higher than 'In-Confidence', sensitive personal information, emails that could adversely affect the reputation of the Commission if they were sent to the wrong person.

- Communications relating to Commission business MUST NOT be sent from public email services (e.g., Gmail, Hotmail) or any method other than approved by the Commission.
- Extra care including checking the recipient address(es), content and attachments are correct SHOULD be taken when sending emails to public email services (e.g. Gmail, Hotmail) especially if the information is 'sensitive in nature'.
- Communications on all Commission communications platforms MUST meet reasonable standards of courtesy. Messages or content that are offensive or discriminatory MUST NOT be included.

Use of Microsoft Teams and Zoom video conferencing

- Microsoft Teams or Zoom video conferencing MUST NOT be used to download, process, store or transmit any material that could be offensive or discriminatory.
- All video conferencing meetings MUST be checked by the organiser before commencing to ensure it includes the correct participants and contains the correct information.
- Users of Teams and Zoom MUST NOT download any unauthorised files to Commission devices.
- If recording any video conferencing meetings, the organiser MUST advise the attendees that the meeting will be recorded and give them the opportunity to object.
- Microsoft Teams is the Commission's default video calling option and should be used by all users when arranging calls. Zoom can be used in an instance where it is the only option and only when the user has read and understood the document "Safely using Zoom for meetings".

Information access

- Access to information stored on Commission systems that is 'sensitive in nature' (such as classified information or Sensitive Personal information/PI) MUST be restricted to only the individuals who require access.
- Any information stored on Commission systems MUST only be accessed for legitimate business purposes, this is regardless of the access permissions configured on the information. For example, if access to a Share Point site or file is unrestricted this does not mean that individuals are permitted to access the information without a legitimate business reason.
- The unauthorised disclosure of the Commission information is subject to New Zealand law including the Privacy Act 2020.

Internet usage

The Commission provides employees with internet connectivity, which is to be used primarily for Commission business. Kaimahi MUST NOT use internet connectivity or Commission information systems to engage in illegal activity such as computer misuse or copyright infringement.

- The Commission uses filtering software to screen out inappropriate or illegal content, as well as logging and monitoring systems to record internet activity. The Information and Technology Services (ITS) team uses logs when responding to an information security incident or investigating unauthorised use of internet connectivity or information systems provided by the Commission. By using a Commission issued device or Internet connectivity you consent to the monitoring of this.
- The Commission operates separate corporate and guest wireless networks. The corporate wireless network MUST only be used by Commission-issued devices. The guest wireless network can be used by visitors or personal devices, including BYO devices.
- To use a Commission wireless network, users MUST enter a pre-shared key (PSK). Kaimahi MUST NOT share the PSK for the corporate network with non-Commission personnel. The guest wireless network PSK MUST only be shared with authorised guests to The Commission.

- When working outside of the Commission office or home office networks, kaimahi SHOULD use the hotspot functionality of their Commission-issued device to access the internet. Public Wi-Fi (such as that in airports, cafes and other locations accessible to the general public) SHOULD NOT be used.

Websites and computer applications

Kaimahi MUST only access Commission information using approved software or web applications (e.g. Share Point) on their Commission-issued device or BYO device. Kaimahi MUST NOT use non-approved software or web applications to view or edit Commission information on any device.

- Web applications that do not have a business purpose (e.g. instant messaging applications) or personal accounts on websites (e.g. a personal email account) MUST be used with care. Do not upload or post anything that could reflect poorly on the Commission, even if this is on a personal account.
- Some websites can be used for personal and Commission business (e.g. social media sites). Use these with care; only post or share content that can be distributed publicly and use privacy settings to limit the availability of your content to other users. Kaimahi can speak to the Information and Technology Services team for more guidance on how to use these kinds of websites securely.
- Remember you are always representing the Commission when using Commission information systems. This includes if you use your Commission-issued device for personal purposes.
- You MUST NOT upload any Commission information to unapproved cloud storage (such as Dropbox or Google Drive), personal email accounts or any other external websites. If you are unsure if a site is approved for use, you MUST first check with the Liquid IT service desk or Manager, Digital Services | Chief Information Officer.
- Kaimahi MUST NOT download or install any application from the internet on a Commission-issued laptop. If a kaimahi member requires an application for business purposes, the kaimahi member MUST place a request with the Liquid IT service desk.

Use of Artificial Intelligence

Use of artificial intelligence tools and services must align with the organisation's AI Policy, which governs the ethical, secure, and responsible application of AI technologies across all business functions.

Authentication credentials

You MUST protect the confidentiality of all authentication credentials that provide access to the Commission information systems by never sharing your credentials with anyone else. This includes usernames, passwords, authentication devices and account information (e.g. secret questions).

- You MUST NOT use your Commission authentication credentials for any other personal sites or systems. The Commission strongly recommends that kaimahi also do not use the same authentication credentials for any personal accounts on websites or applications.

Removable storage media

Removable storage media MUST NOT be used for storing and transferring information between systems.

- This includes copying files to and from USB drives whether these are Commission owned or not. For example, if an external party brings a device into the Commission with a presentation or file to copy to a Commission system this MUST NOT be plugged in.

- Removable storage media access that is required for business purposes may be granted under exceptional circumstances but MUST be authorised in writing by the Manager, Digital Services | Chief Information Officer and Chief Information Security Officer (CISO).

Using mobile devices

You are responsible for the safety of all Commission mobile devices issued to you. This means you MUST take reasonable steps to prevent the device from being damaged, lost or stolen. If loss or damage does occur, you MUST inform the Liquid IT Service Desk and Manager, Digital Services | Chief Information Officer as soon as practicable.

- You MUST not leave mobile devices or laptops unattended in an insecure location. This includes not leaving devices in a locked vehicle overnight and ensuring any devices are hidden from view in a locked vehicle.
- You MUST activate the screen lock on any laptop or mobile device if it is unattended. This applies both when you are onsite at the Commission premises or working remotely.
- Be sensible. You MUST NOT do anything inappropriate on a mobile device that could reflect poorly on the Commission, this includes accessing, downloading, storing or sending any pirated or unlawful software, images, offensive, pornographic or otherwise inappropriate material. Use common sense – if you would normally view it in the office, you can probably view it on your device.

A personal device (e.g. mobile phone, tablet) MUST NOT be used to conduct any Commission business or access any Commission information. The only exception to this is bring your own (BYO) devices, which are personal devices enrolled in the Commission mobile device management (MDM) tool.

- You MUST have approval from your manager and the Manager, Digital Services | Chief Information Officer to use a personal device for Commission business. Your device MUST be compatible with the Commission MDM tool and meet certain minimum technical requirements. The MDM tool will be able to:
  - Remotely wipe any Commission information if the device is lost or stolen. This may result in loss of personal data.
  - Install software onto your device and log actions performed on the device.
  - Require certain settings to be configured on the device (e.g., a passcode or password must be set to unlock the device).
  - Perform regular health checks or similar monitoring of the device.
- BYO devices can only be used to create, store, or transmit Commission information classified as RESTRICTED or below. This includes Commission information exchanged via SMS/MMS or during a phone call.
- Any authentication credentials used to protect the BYO device MUST be different from authentication credentials used to access the Commission information systems.
- You are responsible for the following relating to a BYO device:
  - Keep the device safe from being damaged, lost or stolen.
  - Updating the device's operating system and applications.
  - Any costs associated with the device, including telephone plans, the purchase of accessories or costs incurred when repairing or replacing the device.

- If you leave the Commission or no longer wish to have your device enrolled in the Commission MDM tool, you MUST notify your manager or the Manager, Digital Services | Chief Information Officer and ask the Liquid IT service desk who will commence the process of removing Commission information from your device and unenrolling it from the MDM tool.

Overseas Travel

When travelling overseas whether on Commission business or privately there is an increased level of risk when using information systems including mobile devices and wireless networks.

- If travelling overseas with a mobile device or laptop that can be used to access the Commission systems (this applies to a Commission owned device or BYO device) you MUST consult with the Commission's Departmental Security Officer prior to travelling. This will allow the request to be triaged and escalated.
- If travelling overseas and you want to take your Commission issued device/s, please send a request outlining the country/s visiting and travelling through to security@publicservice.govt.nz.This MUST be done prior to travelling.
- Be aware that you may be unable to take your Commission issued device/s to some countries, based on the risk.

Private use of the Commission's assets

The Commission defines acceptable business use as activities that directly or indirectly support the business of the Public Service Commission. Devices owned or leased by the Commission, such as mobile phones, laptops and photocopiers may be used for personal use. However, the principles of transparency and moderate and conservative expenditure must prevail. We are mindful that Commission resources are publicly owned and funded and we will act responsibly in our use and management of them.

- You MUST use the internet responsibly and productively; reasonable personal use of social networking sites and other websites is permitted providing this does not affect your ability to perform your role. Excessive personal internet browsing, including streaming video or audio, large downloads and social media is not permitted unless connected to a home network.
- You MUST understand and agree that device usage, such as data use, is monitored by the ITS team and if the Commission believes personal use is unreasonable, you may be asked to reduce your non business use or to contribute to the cost.

Printed Information

Printing of Commission information should be kept to a minimum. Where it is necessary to print information, you are responsible for safeguarding the information at all times.

Additional care MUST be taken when printing information that is In-Confidence or above or where disclosure of the information could reflect poorly on The Commission. Good judgement MUST be used as to the document's sensitivity, for example a document may not be classified but it could reflect poorly on the Commission if it was left lying around and its contents were to be disclosed.

For printed information that is In-Confidence or above or where disclosure of the information could reflect poorly on the Commission:

- The information MUST NOT be removed from the Commission premises without being secured in a locked document bag. Locked document bags can be obtained from the Facilities team.
- The information MUST NOT be left unattended (for example on desks or printers) even when in the office.

- The information MUST be secured at all times when outside of the Commission premises office (this includes not leaving documents in a locked vehicle at all and ensuring documents are always secured).
- Information MUST NOT be printed at home or outside of the Commission or other NZ Government secured premises.

Appendix A – RECAP protocol for email sending

The accidental sending of emails or attachments to a person or persons outside of the Commission is one of the most likely drivers of an information security incident at the Commission. The impact of this could be significant and result in potential loss of trust and confidence as well as breaching someone's privacy.

The below protocol has been developed for all kaimahi when sending certain emails and involves having a second set of eyes check certain emails.

Emails subject to the protocol

The emails that are be subject to the protocol are as follows, this is not an exhaustive list and common sense should be applied:

1. Emails that contain information that is 'sensitive in nature' [2]for example CE remuneration details, contracts, CE performance review summary.
2. Emails classified as "sensitive" or above.
3. Emails to external agencies or contacts containing attachments with information that is 'sensitive in nature'.
4. Some emails and attachments require password protection. The following guidance applies:
   a) Emails to another agency sent via SEEMAIL **do not** require password protection. The emails are already encrypted.
   b) Emails with attachments classified 'sensitive' or above to an external recipient (non-public sector) **should be** password protected.
   c) Passwords MUST be sent via an alternative channel (e.g. SMS), **not** via email.

If you have any doubts or are unclear about whether an email is subject to the protocol, consult your Manager.

Email Pre-send Checklist

Prior to sending external emails which meet any of the criteria above, the following checks must be done by a second pair of eyes:

☐ Correct email address, that has been verified by the recipient as appropriate for sharing confidential information.

☐ Appropriate email classification.

☐ Correct attachments and /or hyperlinks.

☐ The appropriate team members are aware of the email (e.g., ACs, and/or Managers).

☐ If the email is password protected, check that the correct password is being sent via an alternative channel.

Note: if you are working remotely, please use Teams screen sharing for a team member to review.

Before sending an external email, **RECAP**:

[2] Discretion should be used when deciding whether information is 'sensitive in nature'. This could include information classified higher than 'In-Confidence', sensitive personal information, emails that could adversely affect the reputation of the Commission if they were sent to the wrong person.

Recipient | **E**mail Address | **C**lassification | **A**ttachment(s) | **P**rotection (if necessary)

If an email and/or attachment is accidentally sent to the wrong recipient:

1. Recall the email and inform your immediate manager (and the Commission Privacy Officer if the email contains personal information).

Appendix B - Artificial Intelligence supporting resources

Office of the Privacy Commissioner

[Office of the Privacy Commissioner | Artificial Intelligence and the IPPs]

Government Chief Digital Officer

[Managing the risks of GenAI to the public service | NZ Digital government]