

09 May 2024

Kia ora [REDACTED]

Your Official Information Act request, reference: GOV-031495

Thank you for your email of 3 April 2024, asking for reports and materials that demonstrate how ACC is, or intends to meet, its commitments under the Algorithm Charter for Aotearoa New Zealand (the Charter).

These commitments are those described in the Charter under the following headings:

1. Transparency
2. Partnership
3. People
4. Data
5. Privacy, Ethics and Human Rights
6. Human Oversight.

Our response

ACC has a number of documents that are relevant to our commitments under the Charter. Our decision is to provide you all ACC documents relevant to this subject. These are as follows:

Document name	type	Where
Huakina Te Rā	ACC's Strategy	www.acc.co.nz/about-us/corporate-documents/our-strategy-huakina-te-ra
How we assess claims	Webpage	www.acc.co.nz/im-injured/how-we-manage-your-claim/how-we-assess-claims
How we use claim information	Webpage	www.acc.co.nz/about-us/how-we-collect-and-use-your-information/how-we-use-claim-information
Creating a new ACC Research Ethics Committee	Media release	www.acc.co.nz/newsroom/stories/creating-a-new-acc-research-ethics-committee
We're using a predictive modelling tool to better support our clients, faster	Media release	www.acc.co.nz/newsroom/stories/were-using-a-predictive-modelling-tool-to-better-support-our-clients-faster
How we use predictive analytics to improve our clients' experience	Media release	www.acc.co.nz/newsroom/stories/how-we-use-predictive-analytics-to-improve-our-clients-experience
How we use algorithms to improve customer experience	Media release	www.acc.co.nz/newsroom/stories/how-we-use-algorithms-to-improve-customer-experience
Generative AI Models and Services Policy	Policy	Attached

It is important to note that many of the objectives that ACC is committed to meet as a signatory to the Charter are or will be embedded into processes and governance structures, rather than contained within specific reports or other materials. For example:

- The Māori Data Governance Group – provides a Māori view as part of governance, and with respect to data issues more broadly.
- ACC's Legal Services and Privacy teams – review all information-related initiatives to ensure they comply with all privacy and legal requirements.

As this information may be of interest to other members of the public

ACC has decided to proactively release a copy of this response on ACC's website. All requester data, including your name and contact details, will be removed prior to release. The released response will be made available www.acc.co.nz/resources/#/category/12.

If you have any questions about this response, please get in touch

You can email me at GovernmentServices@acc.co.nz. If you are not happy with this response, you can also contact the Ombudsman via info@ombudsman.parliament.nz or by phoning 0800 802 602. Information about how to make a complaint is available at www.ombudsman.parliament.nz.

Ngā mihi



Christopher Johnston
Manager Official Information Act Services
Government Engagement

Generative AI Models and Services Policy

POLICY NUMBER	7.0.0
TOPIC	Generative AI Models and Services
OWNER	[Out of Scope], DCE Enterprise Change Delivery
DATE APPROVED	02 August 2023
AUTHOR	[Out of Scope], Head of Information and Technology Integration
DATE OF REVIEW	02 February 2024

1 Objective

The Generative AI Models and Services policy clarifies ACC's stance on the potential usage of Generative Artificial Intelligence (AI) Models and Services at ACC. Generative AI describes algorithms that can be used to create new content, including audio, code, images, text, simulations, and videos.

Our aim is to ensure that this type of technology is used and developed in a responsible, ethical, and sustainable manner which prioritises the long-term well-being of New Zealanders and is aligned with our commitment to The Treaty of Waitangi (Te Tiriti O Waitangi).

This policy aims to strike a balance between enabling innovation and mitigating potential risks. As a principle, we aim to apply reasonable caution, while taking Te Tiriti O Waitangi, privacy, security, and fair labour practices into account.

To achieve these goals, this policy sets out a framework for the responsible use and development of Generative AI Models and Services, including guidelines around transparency, interpretability, privacy, security, and fairness. It also points to the use of appropriate governance structures and procedures, including regular risk assessments, ongoing monitoring and auditing, ethical oversight, and intervention.

2 Scope

This policy applies to:

- all ACC people, including employees, secondees, accredited employer providers, and independent contractors (ACC staff)
- all Generative Artificial intelligence (AI) Models and Services (Generative AI Models and Services), and
- all data types, including all ACC intellectual property (IP), data sets, and personally identifiable information (PII).

This policy is supplemented by the Security, Information Management, Personal Information, social media and Privacy policies and guidelines, which further detail how we appropriately collect, store, use, disclose, and retain various categories of information.

This policy also recognises the potential risks associated with the use of Generative AI Models and Services, including the potential for biased or discriminatory outcomes, the generation of offensive or harmful content, and the displacement of human workers. To mitigate these risks, this policy places a strong emphasis on alignment with Te Tiriti O Waitangi, the protection of user privacy, personal information and intellectual property rights, and the promotion of work standards that ensure fair and equitable treatment of ACC's people.

At the same time, this policy recognises that the responsible use and development of Generative AI Models and Services can have a positive impact on ACC's services and people, including promoting access to information, uncovering insights and knowledge, fostering innovation, and promoting creativity which could result in positive outcomes for ACC. By adhering to these principles and guidelines, ACC can endeavour to ensure that its use of Generative AI Models and Services is aligned with ethical and responsible principles, while also promoting the protection of user privacy, the promotion of fair workplace practices, and the potential advancement in the ways we work to deliver our strategy.

3 Policy Statements

Context

This policy is underpinned and informed by:

- the principles and rules of the *Privacy Act 2020 and the Health Information Privacy Code 2020* which govern how agencies manage personal and health information throughout the information lifecycle (collection, storage, access, correction, use, disclosure, and disposal)
- the Algorithm Charter for Aotearoa New Zealand
- the Data Protection and Use Policy
- the Crown's commitments to Māori under Te Tiriti o Waitangi, and
- the Government's Protective Security Requirements.

Policy statements

1) Transparency is at the forefront of any Generative AI usage.

ACC's staff are transparent about their use of Generative AI Models and Services and their capabilities, including any potential limitations or biases, to promote trust and transparency with ACC clients and third parties.

2) ACC will have human oversight included throughout the use of any Generative AI Model.

In all cases, human oversight must be in place throughout and at the conclusion of the use of any Generative AI Model or Service to monitor outputs and intervene if necessary to ensure the output is accurate and the technology is being used ethically and responsibly.

3) Data privacy and security are paramount.

All Generative AI Models and Services should be used, designed, and developed with privacy and security in mind, and appropriate security controls and measures should be implemented to protect against cyber threats and unauthorised access or sharing of information in line with our enterprise risk appetite statements.

4) ACC will actively protect Mātauranga Māori, tikanga, and taonga (Māori Protected Materials).

Māori Protected Materials must not be entered into Generative AI Models and Services, where doing so could threaten the integrity of the materials, Māori control over the materials, or the cultural, economic, or other potential to Māori of the materials. This is particularly important where an AI Model or Service may 'learn' from or interpret the materials and add them to its corpus of knowledge. Internal and/or external Māori advisors must be consulted before such materials are entered into Generative AI Models and Services.

5) We will comply with all applicable laws and associated policies.

ACC's staff will ensure that the use of any Generative AI Model or Service is compliant with applicable laws and ACC policies, including by ensuring that Privacy and Ethics Risk Assessments are done, and that user data is protected through appropriate data privacy and security safeguards, as per ACC's Privacy, Information Management and Security policies.

6) All Generative AI Models and Services must have a focus on ethical use.

ACC's staff are aware of the potential for bias or discrimination in any Generative AI Model outputs and will take steps to mitigate these risks through taking ethical considerations into account when using existing AI tools and when developing, testing, and third-party auditing other tools. All structured uses of Generative AI Models and Services at ACC must be reviewed by the ACC Ethics Panel via the Privacy and Ethics Risk Assessment process prior to implementation or use.

7) We will collaborate with relevant stakeholders when considering or using Generative AI Models and Services.

ACC's staff will collaborate with relevant stakeholders, including internal and external experts in Generative AI ethics, security, and privacy, to ensure that Generative AI Models and Services are developed and used in a manner that benefits New Zealanders.

8) Clarity on usage purposes.

ACC's staff will provide clarity and decision-making processes for the use of any Generative AI Models and Services. ACC's staff will ensure we use Generative AI Models and Services in line with ACC's objectives.

9) We will consider and take reasonable steps to protect and respect ACC and third-party intellectual property rights.

Inputting ACC or third-party intellectual property into a third-party Generative AI Model or Service may put the owner's ownership of the intellectual property rights at risk.

ACC staff should not enter ACC or third-party intellectual property into third-party Generative AI Models or Services if doing so would put ACC's intellectual property at risk or infringe third-party intellectual property rights.

On the output side, ACC recognises that there are unresolved legal issues regarding the materials on which some large language models have been trained, how they generate their outputs, whether the outputs are protected by intellectual property laws and, if so, who owns the relevant intellectual property comprised in such outputs.

ACC staff should not:

- use or publish outputs generated by Generative AI Models or Services (particularly images, audio, music or video) where doing so would raise a real risk of infringing third-party intellectual property rights; and
- use external Generative AI Models or Services for the development of business outputs or tools (such as software, software applications) for use in ACC's business, if ACC's ownership of, or right to use the intellectual property rights comprised in such outputs or tools cannot be assured.

10) We will always follow guidelines.

By following these guidelines, ACC's people can help ensure that the use and development of Generative AI Models and Services is secure, ethical, and responsible, while also promoting transparency and trust with users.

4 Generative AI Models and Services usage guidelines

Below is a brief list of guidelines for the use of Generative AI. Please see the associated Generative AI Models and Services Guidelines for a descriptive list of acceptable and unacceptable use which is also supplemented with case study examples.

- Anyone who uses Generative AI Models and Services must comply with the terms and conditions of use of the Generative AI Model or Service.

- ACC staff must not sign up to terms and conditions on behalf of ACC without manager approval and, where required, CISO approval to the use of the cloud services.
- Generative AI Models and Services use may only be used for purposes which are not related to client care and do not involve the entry of any personal or health information. Examples may be draft document creation for internal reports, creation of marketing materials or for help with excel code when creating a visualisation.
- New uses must be approved by the Security, and Privacy and Ethics Risk Assessment processes prior to implementation. Usage cannot begin until these assessments are signed off.
- Do not use external Generative AI Models and Services for activities which determine care or resourcing provided to clients, customers, or providers. All statutory decision making must be made in accordance with ACC's Corporate Delegations Framework.
- When in doubt over the usage of Generative AI Models and Services, check with the Ethics and/or Privacy Team if the proposed usage is acceptable. Questions or concerns relating to intellectual property usage should be directed to the ACC Legal Team.
- Do not enter any client information, personal data, confidential content, or ACC intellectual property into third-party Generative AI Models or Services if that model/service will learn from it or store it outside our tenancy.
- Generative AI outputs can be unreliable. You must review and approve all outputs created by Generative AI Models and Services before sharing or acting upon them. Test proposed evidence-based results by independently checking references and evidence for validity.
- Regularly back up all data processed through Generative AI Models and Services to minimise the risk of data loss.
- Comply with all applicable data protection, information management, privacy, security, and IP laws, regulations and policy.
- Report any misuse or potential privacy or security incidents involving Generative AI Models and Services to your manager.

5 Accountabilities

Board responsibility for information management is set out in our Board Governance Manual and this includes the use of data as an input to any Generative AI Model or Service. This acknowledges that the Board is committed to ethically managing personal and health information by:

- Setting clear expectations regarding ethical use, privacy, and protection of personal information, and communicating them to the executive management.
- Holding executive management accountable for meeting those expectations.

- Ensuring effective privacy and information risk management is fully embedded within our overall risk management activities.
- Implementing high-quality monitoring and information management practices.

Our managers are directly accountable for identifying and addressing information and data risks in their own units to ensure these are captured for reporting to the Board via the appropriate channels.

All members of the Executive are responsible for driving strong enterprise-wide culture and practices for the care, ethical use, and protection of personal information.

The Deputy Chief Executive (Enterprise Change Delivery) on behalf of the Executive, is accountable for ensuring supporting guidelines, operational measures and monitoring practices are in place.

6 Roles and Responsibilities

Role	Responsibility
Head of Information and Technology Integration	<ul style="list-style-type: none"> • Ensures policies reflect relevant legislative or regulatory requirements, rules, standards, and codes that apply to ACC. • Ensures policies include monitoring and oversight mechanisms that reflect the principles of the 3 Lines of Assurance. • Ensures policy content is accurate, relevant, complete, and aligned with other related policies and the Corporate Policy Governance Framework. • Liaises with subject matter experts and relevant groups and committees, including the Enterprise Risk Team and external shareholders (for example: NZ Public Service Association) • Ensures policies are communicated, and training activities and guidance documents are in place to support implementation of the policy. • Ensures mechanisms are in place to monitor compliance with our Generative AI Models and Services Policy. • Considers and, if appropriate, approves policy exceptions. • Responds to, and addresses, any non-compliance issues and ensures processes are in place to identify, manage, record and report policy breaches and exceptions as appropriate. • Ensures policies are reviewed within a six-monthly cycle or as otherwise required.

Head of Privacy	<ul style="list-style-type: none"> • Reviews and approves requests to extend the use cases for new AI Models and Services via the Privacy Risk Assessment process. • Supports the ongoing review of AI-related research, quality improvement activities and data requests in ACC via the Ethics Panel. • Ensures support is available for AI-related ethical decision making
Role	Responsibility
	<ul style="list-style-type: none"> • Provides reporting to the Executive and Board on AI related Privacy breaches as appropriate.
ACC Legal Team	<ul style="list-style-type: none"> • Provides legal advice and assurance, as required
1st Line of Assurance	<ul style="list-style-type: none"> • Managers, People Leaders, and all ACC's people should ensure appropriate processes and activities are in place to track compliance. • Each policy should include monitoring and oversight mechanisms that follow the principles of the 3 Lines of Assurance. <p>People Managers have specific responsibilities for:</p> <ul style="list-style-type: none"> • Notifying Generative AI Model or Service-related incidents to their manager. • Proactively assessing and managing Generative AI Model or Services risk. • Where necessary, liaising with the relevant group (People and Culture, Integrity, Security, or Privacy) following Generative AI Model or Services incidents to ensure consistent follow up with ACC's people. • Updating and managing the unit's Risk Register and ensuring it is kept current. • Ensuring ACC's people are aware of, and recognise, the importance of their role in Generative AI models and Services usage. • Ensuring ACC's people are aware of and compliant with our Information Management, Personal information and Privacy, and Information Security Policy, the Privacy Act 2020, the Health

	<p>Information Privacy Code 2020 and complete their annual compulsory training.</p> <ul style="list-style-type: none"> Ensuring new staff induction includes Generative AI Model and Services usage information.
Our People	<ul style="list-style-type: none"> Comply with this policy.

7 Monitoring and oversight

Our Generative AI Models and Services Policy and Generative AI Models and Services Guidelines have been developed to be consistent with the Privacy Act 2020, the Health Information Privacy Code 2020, and the Health Information Security Framework (HISF) 2022.

The monitoring and oversight of Generative AI Models and Services follows the 3 Lines of Assurance model to provide assurance that staff and third-party privacy risks are being managed effectively.

Line of Assurance	Role	Responsibility
1st Line	Employees and People Leaders	<ul style="list-style-type: none"> All employees: <ul style="list-style-type: none"> Remain alert to potential breaches of the Generative AI Models and Services Policy and report potential and actual breaches to their manager. Maintain best Generative AI Model and Services usage behaviours, promote privacy at work, comply with privacy, security, and information management policies, actively participate in training, and identify associated risks. All people managers ensure: <ul style="list-style-type: none"> Generative AI Models and Services policy breaches and incidents (near misses etc.) brought to their attention are documented appropriately, Notification of the breach is provided to the Privacy Team within 24 hours of the breach occurring, and They act to resolve the breach in a timely fashion, obtaining guidance and support from the Information management and/or Privacy Team and/or Legal Team as/when required.

	Head of Information and Technology Integration	Ensures ACC responds appropriately to Policy breaches and requests for exceptions.
Line of Assurance	Role	Monitoring & Oversight
2 nd Line	Enterprise Risk Team	<ul style="list-style-type: none"> Performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of Generative AI Models and Services usage practices to monitor compliance and deal with breaches. Reports to the Executive and the Board on the outcomes of such activities via the quarterly risk report.
3 rd Line	Internal Audit (and external providers)	<ul style="list-style-type: none"> Perform periodic audit activities intended to assess, and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of ACC's practices to monitor compliance and deal with breaches. Report to the Executive, Risk Assurance and Audit Committee (RAAC) and Board on the outcomes of such activities.

8 Breaches of Policy

We require any potential or perceived Generative AI Model or Service incidents to be reported to management as soon as reasonably practicable, and in all cases, within 24 hours of awareness of the incident. This includes incidents that have been observed or directly contributed to.

Our Code of Conduct requires our people to comply with all our policies. Breaches of this policy can result in a range of consequences for our people, for ACC and our clients.

While we strive to be good guardians of personal information, incidents will happen. When they do, our priority is to make things right. Accidental failures to achieve the standards in this policy will not normally be grounds for disciplinary action. Repeated, deliberate, or negligent failures (including by failing to report an incident) may result in disciplinary action.

9 Relevant related Policies and Guidelines

[Use of the Internet Policy](#)

[Cloud Computing Policy](#)

[Code of Conduct](#)

[Personal Information and Privacy Policy](#)

[Social Media Policy](#)

[Information Management Policy](#)

[Information Security Policy](#)

[Generative AI Models and Services Guidelines*TBC](#)

10 Contacts

For any enquiries about issues of interpretation or management of the policy please contact the [Information Management team](#)

11 Version Control

Version	Date	Change reason	Who
0.1	02/08/2023	Full update	[Out of Scope]
0.2	03/10/2023	Policy review date updated	[Out of Scope]
0.3	14/12/2023	Minor updates from reviews	[Out of Scope]