ACC Privacy Impact Assessment (PIA)

Agent Copilot

March 2025

Overview

This privacy impact assessment (PIA) evaluates the privacy implications and risks of Accident Compensation Corporation using Agent Copilot, an AI-powered assistant will help Service Delivery team members assist ACC customers faster and more efficiently. It will cover the following aspects:

• The purpose and scope of the project, and the objectives for using Agent Copilot at ACC.

• The compliance with privacy principles and legislation, under the Privacy Act 2020 and the Health Information Privacy Code 2020, and the identification and mitigation of any potential gaps or risks.

• The jurisdictional and legislative analysis of the different laws and regulations that may apply to the data collected and processed by Agent Copilot, including international privacy legislation.

• Privacy and Generative AI policies and guidelines that will be applied to the use of Agent Copilot at ACC.

• The data collection and processing activities that will be performed by Agent Copilot, and the types and sources of personal and sensitive health information that will be involved.

• The ethical concerns associated with using Agent Copilot at ACC.

• The privacy risks and challenges that may arise from using Agent Copilot at ACC, and the actions and measures that will be taken to prevent and contain privacy risk.

• The benefits evaluation of implementing Agent Copilot at ACC, and the evidence and examples of how it can positively impact the productivity, call resolution, and average handle time of contact centre and frontline teams.

• The conclusion and recommendations for using Agent Copilot at ACC, and the areas for improvement and further discussion.

The PIA is based on the information and guidance provided by ACC, Genesys, and other relevant sources. The PIA is intended to be a living document that will be updated and reviewed regularly, as the project progresses, and new information or changes emerge.

Background and approach

ACC's Service Delivery teams are currently bound to business processes that can be transformed using modern-day technology, and there are opportunities to invest in their technology to create efficiencies and remove manual handling.

One opportunity to reduce the handle time for voice interactions and improve the 'speed to competency' in our Contact Centre is a capability within our existing Genesys Cloud platform called "Agent Copilot."

Agent Copilot uses assistive AI technology that streamlines customer calls/interactions with the following use cases:

1. **Advanced summarisation**

   Agent Copilot generates an automated summary of the interaction at the end of a phone call, allowing staff members to edit the summary for accuracy & then paste it in the system of record, reducing the time spent on after call work. Reducing time spent in After call work (ACW) will create an improvement of 'Average Handle Time' (AHT), resulting in less time spent on hold by our clients and increased efficiency for all team members augmented with this assistive AI capability.

2. **Generative knowledge**

   Agent Copilot also provides the ability to automatically surface relevant knowledge material from Genesys Knowledge Workbench to our staff members working on both voice & digital channels.

   Genesys will surface knowledge material that has been summarized and contextualized to the question asked by the caller. This ensures all staff members within our contact centre deliver consistent, accurate information for all interactions and can greatly improve the 'speed to competency' when training new staff members, whilst also reducing internal consultation with Channel Support Advisor (CSA's).

Scope and current/future state

The scope of this document covers the use of Agent Copilot at ACC for the Contact Centre and other frontline Recovery teams. The approach to its rollout is phased. This allows ACC to formulate controls to mitigate privacy risk identified during lab and small group testing prior to rolling the technology out to a wider user group.

The purpose of completing a PIA is to identify the impact that using Agent Copilot within ACC may have on privacy. Further to this, it will identify mitigations that can be put in place to ensure that the privacy risks identified are addressed pre-emptively.

Initial Testing and Feedback

Genesys Copilot will be rolled out in a considered approach. Initially, functionality will be tested in a lab environment, followed by testing with a small group of 30 Contact Centre users in the production environment.

Rollout of Genesys Agent Copilot across ACC

Following user acceptance testing with a small group in the production environment, the rollout will start with approximately 300 Contact Centre users and then extend to other many-to-many recovery teams. Change management, communication, and training will accompany the rollout to ensure users and customers benefit from the tool.

The generative knowledge functionality will query the Genesys Knowledge workbench knowledge articles from the Vault in the first instance but may be extended/replaced by other knowledge sources like SharePoint in future, depending on the future direction and optimisation of frontline knowledge.

It is important to note, that the scope of this PIA is limited to the Genesys Agent Copilot. The scope does not include the general telephony functionality of Genesys Cloud which is already in use at ACC.

Privacy and legal frameworks relevant to this PIA

New Zealand - Privacy Act 2020

The Privacy Act 2020 forms the basis of the risk analysis matrix used to assess the privacy implications of Accident Compensation Corporation using Agent Copilot. The Information Privacy Principles (IPPs) which set out legal requirements on how you collect, use, and share personal information need to be considered when using AI tools. The IPPs apply to each stage of building and using AI tools – in the case of Agent Copilot, those stages are taking user input, receiving a response, and acting as a result. ACC have a wide range of statutory functions and duties under the Accident Compensation Act 2001. ACC collect, use, store and share personal information to fulfil those functions and duties and are therefore required to comply with the principles in the Privacy Act 2020.

New Zealand - Health Information Privacy Code 2020

ACC's use of Agent Copilot must comply with the Health Information Privacy Code (HIPC) which sets specific rules for agencies across New Zealand's health sector. Of particular relevance is Rule 5 of the Code requires health agencies to take 'reasonable security safeguards' to protect health information. This means keeping health information safe from loss, as well as from unauthorised access, use, modification, or disclosure.

United States of America - US CLOUD Act 2018

The Clarifying Lawful Overseas Use of Data (CLOUD) Act is a United States federal law primarily amending the Stored Communications Act of 1986 to allow federal law enforcement to compel USA based technology companies via warrant or subpoena to provide requested data stored on servers, regardless of where the data is stored. Data is securely stored in ACC's Genesys cloud AWS environment which is located within Australasia but as the parent company is American, falls under the jurisdiction of this act.

European Union Artificial Intelligence Act (EU AI ACT) 2025

The EU AI Act is a regulation that will come into force in 2025 that that aims to ensure that AI systems used in the EU are safe, trustworthy, and respect fundamental rights and values. This regulation will apply a risk-based approach, with stricter rules for high-risk AI systems, such as those used in health care, law enforcement or critical infrastructure. The proposed EU AI Act can apply extraterritorially to providers from outside the EU if they have products within the EU. Meeting these regulations would be an obligation on Genesys if or

when they expand products within the EU, but ACC would need to review any impact the regulations have on the functionality or risk profile of Agent Copilot and adjust their use of it accordingly at that time.

Policies and guidance relevant to this PIA

Data Protection and Use Policy

ACC's use of Agent Copilot will be required to conform with the principles and guidelines of the Data Protection and Use Policy which relate to the respectful, trusted, and transparent use of personal information. Principles from the Data Protection and Use Policy are integrated into ACC's Generative AI Models and Services Policy which can be seen in Appendix 1.

Office of Privacy Commissioner Generative Artificial Intelligence guidance

In June 2023, the Office of Privacy Commissioner published guidance for the use of generative Artificial Intelligence (AI) by agencies. This guidance states that agencies need to be aware of potential privacy risks that have been associated with these tools. These risks include:

- The privacy risks for training data used by generative AI (They also strongly caution against using sensitive or confidential data for training purposes).
- Confidentiality of information entered by generative AI.
- Accuracy of information created by the generative AI.
- Access and correction to personal information.

This PIA addresses these risks in relation to Agent Copilot.

The Office of the Privacy Commissioner expects that agencies considering implementing a generative AI tool will:

- Have senior leadership approval.
- Review whether a generative AI tool is necessary and proportionate.
- Conduct a Privacy Impact Assessment.
- Be transparent.
- Engage with Māori.
- Develop procedures about accuracy and access by individuals.
- Ensure human review prior to acting.
- Ensure that personal or confidential information is not retained or disclosed by the generative AI tool.

Public Service AI Framework

The public service AI framework is guidance relating to and supporting responsible use of AI technology in the public service. Agencies are encouraged to align with the directions set by this framework to ensure safe, best practice AI use.

The five principles that the framework is based around are:

- Inclusive, sustainable development
- Human-centred values
- Transparency and explainability
- Safety and security
- Accountability

Algorithm Charter

The Algorithm charter for Aotearoa New Zealand demonstrates a commitment to ensuring New Zealanders have confidence in how government agencies use algorithms. ACC is one of the signatories of this charter, by signing the charter ACC commits to applying the algorithm charter commitments as guided by risk ratings.

The 6 commitments of the charter are:

- Transparency
- Partnership
- People
- Data
- Privacy, ethics, and human rights
- Human oversight

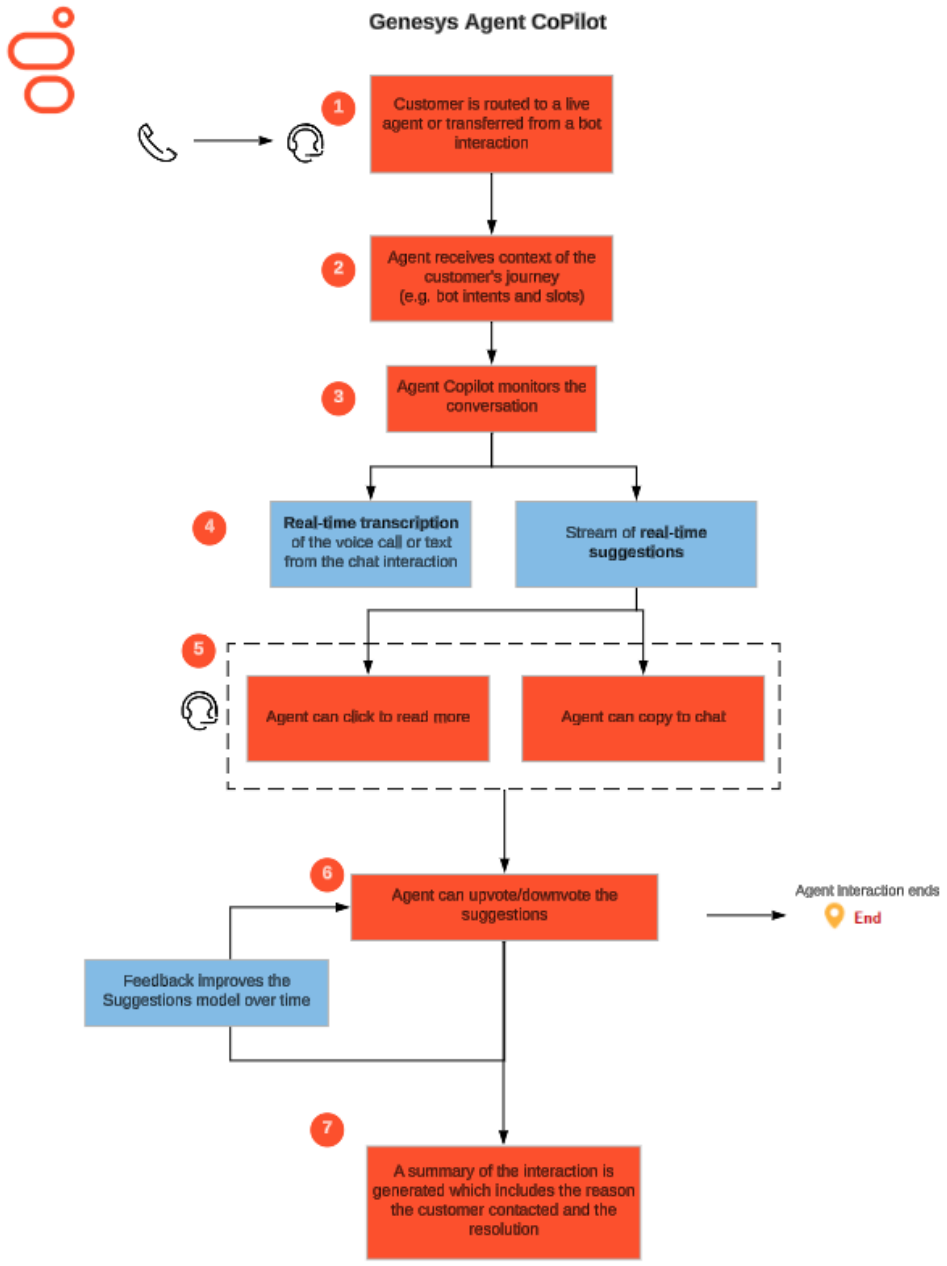
ACC Generative AI Models and Services Policy

ACC have a policy in place which clarifies ACC's stance on the use of Generative AI models and services at ACC. The 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. The policy statements that ACC will adhere to are summarised below (the full statements can be found in Appendix 1): We discuss some aspects of these statements and how we have acted in

accordance with them in our discussion of ethical issues and controls that we have in place.

1. We are transparent about all Generative AI usage.
2. We always have human oversight throughout the use of Generative AI Models or Services.
3. We will make data security and privacy paramount in the design and use of Generative AI Models and Services.
4. We will actively protect Mātauranga Māori, tikanga, and taonga (Māori Protected Materials).
5. We will comply with all applicable laws and associated policies.
6. We will apply an ethical lens to all Generative AI Models and Services use.
7. We will consider and take reasonable steps to protect and respect ACC and third-party intellectual property rights.
8. When an incident or breach occurs, we fix it and learn from it.

How Agent Copilot works



1. Genesys connects the user to the live staff member.
2. The staff member sees the context of the user's journey in the agent desktop.
3. Agent Copilot monitors the conversation.
4. During the voice conversation, the following happens:

For Voice Interactions:

- Real-time audio of the voice interaction is streamed to Genesys Transcription service.
- Agent Copilot displays the real-time transcription of the voice call.
- Agent Copilot uses Natural Language Understanding to understand Customers Intents.
- Agent Copilot service returns real-time next best actions (knowledge, Canned Response or a script)
- The suggested action is displayed to the staff member automatically in a live stream of suggestions during the conversation.

5. The staff member can do the following with the live stream of suggestions:
    - Click to expand knowledge suggested content to read more.
    - Click to launch suggested Script pages to follow a script.
    - Click to expand Canned Responses.
6. The staff member can rate (upvote/downvote) to improve the AI suggestions model over time. The more that Agent Copilot is used and content rated by staff members, the better the suggestions will be in the future.
7. When an ACC staff member ends the interaction with the customer, Agent Copilot offers the staff member a summary of the interaction. Staff members can review the summary and then add them to wrap up notes. In addition, the advanced summary fields are populated which includes a suggested wrap up code, the reason for contact and resolution.
8. The Contact Centre staff member/ frontline team member will need to review the AI generated summary to ensure that the summary of the call is an accurate reflection

of the discussion, edit the summary as necessary and upload it to the customer record in EOS/Salesforce.

Artificial intelligence usage and models

Agent Copilot uses multiple forms of AI including conversational, generative, and predictive AI to enhance interactions through transcription, insight extraction, and summarization. Semantic search enables intent-based information retrieval. It uses a combination of Genesys native and AWS Bedrock models depending on the feature, use case, and language.

Amazon Bedrock provides foundation models (FMs) via a unified API for text generation, classification, question answering, and summarization. The answer highlighting algorithm uses an Open Source LLM model (FLAN-T5) for English and Spanish, generating summaries that capture key dialogues. AWS Bedrock foundational models, such as Claude Haiku by Anthropic, are used for other languages.

All LLMs are hosted within the Genesys Virtual Private Cloud (VPC), and data does not leave this secure environment.

Agent Copilot utilizes different AI models for various functionalities (discussed here):

- **AI Search, Knowledge surfacing and Knowledge Answer Highlight:** Open Source LLM Model (FLAN-T5) for English and Spanish, and AWS Bedrock models such as Claude Haiku.
- **Voice Transcription Services:** Conformer Model, combining Transformers and Convolutional Neural Networks (CNN).
- **Intent Miner:** POS tagger and dependency parser inputs for embedding generation and custom clustering algorithm.
- **Intent Identification:** Uses word embeddings and TF-IDF vectors for classifier input features, enhancing detection with a neural network-like dictionary model.
- **Conversation Summarization and Advanced Summary Fields:** Generative AI automatically creates interaction summaries. Open Source LLM Model (FLAN-T5) for English and Spanish and AWS Bedrock models like Claude Haiku.

Data used for training AI models

The models used in Agent Copilot are trained using knowledge articles, open-source conversations, and anonymised customer-donated conversations, with mechanisms in

place to reduce bias, ensure data quality, and maintain data security. ACC does not share/donate any data with Genesy for the training of AI models.

Agent Copilot: Data Collection and Processing

All functionality of Agent Copilot is 1st party. This means that data remains within the ACC's Genesys environment in the Australian Amazon Web Services data centre, and security and privacy are strictly governed by the standard Genesys Cloud protocols. Agent Copilot does not access any web content.

Genesys Cloud uses Hypertext Transfer Protocol (HTTPS) and Transport Layer Security (TLS) to secure all connections to browsers, mobile apps, and other components bi-directionally with Advanced Encryption Standard (AES)-256 encryption.

Genesys Cloud encrypts voice traffic with TLS Session Initiation Protocol ((SIP) signaling) and Secure Real-Time Transport Protocol (SRTP) (IP voice). Call recordings are encrypted in transit and rest.

ACC's Genesys environment has instances of the LLM's used by Agent Copilot - meaning queries, prompts and responses do not move outside our technical and geographic boundaries.

Voice Transcription Service

Genesys's Voice transcription service underpins Agent Copilot, converting voice interactions into speaker-separated text. Using its native transcription for designated queues, Genesys Cloud employs linguistic and acoustic models to transcribe voice to text.

Whilst the staff member is on a call, real-time audio of the voice interaction is streamed to the Genesys Transcription service and displays the real-time transcription of the call. This forms the foundation for Agent Copilot's other functionality.

The voice transcription service works with the Dictionary to improve the accuracy of the transcription used by Agent Copilot. The Dictionary includes a list of organisation-specific terms, example phrases, alternative spellings and dialects that can be configured by administrators.

Voice transcription offers automated redaction of sensitive personal information, such as names, surnames, and credit card details. However, to ensure the accuracy of records

against the claim in EOS/Salesforce, personally identifiable information (PII) in the transcript or summary will not be auto redacted.

Conversation Summarisation

After an interaction, Genesys Agent provides an automated summary of the interaction for staff to review and add to wrap up notes. It also includes advanced summary fields with suggested wrap up codes, contact reasons, and resolutions.

Data sources for auto summarisation can be voice call transcriptions or chats from digital channels/chat and is sent to the LLM for processing to produce the summary.

The LLM that provides the summarisation service does not retain the conversation or summary once the data has been returned to the staff member. Staff will be required to review the summary for accuracy prior to uploading it to the customer record in EOS/Salesforce. The auto-generated summary is stored in Genesys for 10 days.

To measure the effectiveness of Agent Copilot for summarisation, staff performance metrics such as Average Handle Time and After Call Work are available in the Genesys performance dashboards and will be monitored against metrics pre-rollout. Speed to competency of new staff will also be measured.

Generative knowledge

Knowledge articles stored in Genesys Cloud are used to provide answers and suggestions to the staff member based on the content and intents of the conversation with customer. These knowledge articles are guides for servicing ACC customers and do not contain any PII.

Agent Copilot offers the following functionality for optimising knowledge surfacing to staff in interactions:

- **Knowledge AI generated answers:** Agent Copilot lets staff members search for articles manually and provides real-time summaries from the highest confidence article.
- **Knowledge surfacing:** The AI algorithm uses similarity and semantic search to find the most relevant knowledge articles for the customer's query. The LLM processes document titles, phrases, and content and shows the relevant knowledge articles

to the staff member in real-time but does not make decisions nor sends anything to the customer. The staff member can choose whether to use the suggested knowledge article.

- **Knowledge Answer Highlight:** Agent Copilot can highlight the most important part of knowledge articles for quicker staff access. The same models used to find relevant articles also highlight key phrases. Staff members can always view the full article or summaries and decide whether to use them in the interaction.

To measure effectiveness of generative knowledge, Knowledge Optimiser allows knowledge administrators/authors to measure how well knowledge articles are working including feedback from staff.

Canned responses

Canned responses are pre-written answers to commonly asked questions that staff members can use during an interaction. If Agent Copilot detects a trigger or an intent in the customer's messages, and your administrator assigned a canned response to that trigger, then the assigned canned response appears in the Copilot panel.

Scripts

Scripts guide staff members through an interaction. Scripts can be simple or complex and can consist of one or multiple pages which can contain information about a contact, prompts to read and instructions to follow.

If Agent Copilot detects a trigger or an intent in the customer's words, and an administrator has assigned a script to that trigger, then Agent Copilot will display the 'Load script' button next to the transcribed message.

While in the conversation, the Copilot also suggests various interactions with the loaded script, based on the context.

How does ACC protect client information across Agent Copilot use?

Agent Copilot's knowledge capabilities use knowledge articles in Genesys that do not contain any PII and is centrally controlled by administrators / knowledge managers. Genesys Copilot does not have access to web content.

Voice transcription and auto-summaries will contain a customer's personal information discussed in the call/interaction. This could include Name, Surname, ACC number, medical conditions, provider details and other data.

Data is only stored for a set amount of time and is stored securely in ACC's Genesys cloud AWS environment.

Access, security, and user training measures will be implemented to protect the PII in transcripts and auto-summaries which are discussed in the technical and non-technical controls sections below.

ACC Technical Privacy Controls

ACC has implemented several technical, access and retention controls to help protect its data and apply permissions to Agent Copilot functionality. This includes:

Knowledge articles:

- Administrators / Knowledge managers in the Contact centre manage knowledge articles for content accuracy, and only they have access to do so.
- No access to Web content.

Voice transcription:

- Staff members will only have access to their own calls.
- Team leaders have access to their staff members calls for quality assurance.
- The full call transcription is retained for 90 days, in line with our current call recording retention. The transcription used by Genesys Copilot for the auto-summary is discarded after the call.
- Data is securely stored in ACC's Genesys Cloud AWS environment.

Auto-summaries

- The LLM does not retain the conversation or summary once the data is returned to the staff member.
- Data is securely stored in ACC's Genesys Cloud AWS environment.
- The summary of the interaction is only retained in Genesys for 10 days.
- Staff members will be required to review generated summaries for accuracy and if needed, modify them prior to saving it and uploading it to the system of record.
- Future functionality will include staff members ability to submit positive or negative feedback on summaries presented and for supervisors to view and analyse auto-generated summaries.

Access to Agent Copilot

- Only Administrators can configure call queues and staff members' access for Agent Copilot.
- Training will be provided to staff members prior to given access, both to use the tool but also to review auto summaries for accuracy and potential bias.

- Our sensitive claim lines will not be included for transcription and summarisation, this aligns with our policy on call recordings on these lines

ACC non-technical privacy controls

Education and training

Agent Copilot risk awareness will be incorporated within the toolset training for staff, to ensure inconsistencies from auto summaries are recognised and handled by a human (Staff member) during the editing of the summary notes.

As part of assessing their performance all contact centre staff and recovery team staff have monthly reviews of their calls and this will be ongoing after Agent Copilot has been introduced. Quality of staff members summaries will be monitored over time and can be compared to pre-rollout summaries.

They will also be asked to familiarise themselves with, and abide by, ACC's Generative AI Models and Services Policy and Guidelines.

Human oversight

Human oversight is required as part of ACC's Generative AI models and Services Policy (see Appendix 1). A key control to ensure accuracy & relevance of the summary produced by Agent Copilot is human intervention. The staff members role will change from authoring the notes, to reviewing and editing summaries for accuracy, prior to uploaded to the system of record.

Users will undergo training on ways to review information produced by Agent Copilot.

Applying relevant policies and guidelines

ACC will apply relevant policies and guidelines as outlined in pages 8-9 of this document. Adherence to these policies will be monitored and governed by both the ACC Genesys Cloud Product Owner, the ACC Information Governance Group, and the Generative AI Working Group

Appling the NIST frameworks

ACC has adopted three key National Institute of Standards and Technology (NIST) frameworks for risk management purposes:

1. NIST Cybersecurity Framework – this provides comprehensive guidance and best practices to improve information security and cybersecurity risk management. This framework is fully implemented

2. NIST Privacy Framework – a tool for improving privacy through a qualitative approach to enterprise risk management. This has been partially implemented, implementation of this framework is ongoing.

3. NIST AI Risk Management Framework - In collaboration with the private and public sectors, NIST has developed a framework to better manage risks to individuals, organisations, and societies associated with artificial intelligence (AI). Released by NIST in January 2023, this framework was introduced to ACC later in 2023.

ACC is the first organisation in New Zealand to operationalise the NIST AI Framework, as well as the first organisation to have all three of these frameworks working together to protect people, data, processes, and systems.

Overall, implementing the NIST framework for AI has allowed ACC to map controls for risks arising from the use of Generative AI. In addition to the risk controls covered in the above sections the ACC Product Owner for Genesys Cloud will provide input to ACC's six-monthly AI Risk Management Process Review and annual AI Stakeholder Engagement Process review.

They will also reassess Agent Copilot and user guidelines and training if the ACC Information Governance Group make changes to ACC's approach to Generative AI based on legislative or regulatory changes.

See Appendix 2 for a table of ACC's Generative AI risk controls that relate to Agent Copilot, and information on how these will be addressed.

Ethical Concerns

The following is information and advice given during the ACC Ethics panel meeting regarding this project.

- The Panel queried whether kiritaki consent to the use of Genesys Agent Copilot. The Panel noted that a message on ACC's website that AI was being used would not qualify as a person giving consent. The Panel recommended putting further information about ACC's AI use on the ACC website and considering putting a message at the start of a call.
- The Researcher noted that kiritaki are unable to opt out Copilot being used on a call, as it cannot be switched off. The Panel suggested that if kiritaki expressed concern that generative AI would summarise their conversation then kaimahi could offer not to use the summary as a starting point to write their contact notes.
- The Panel noted the importance of transparency and suggested that ACC's guiding principles around the use of generative AI be shared. The Panel noted that the Algorithm Charter requires transparency.
- The Panel asked what kind of peer review summaries would undergo. The applicant noted that all kaimahi would be expected to review and edit summaries to ensure that they were an accurate representation of the call. Some summaries could be reviewed for second time, for example when kiritaki used Te Reo Māori and the kaimahi were not certain that what had been summarised had been recorded correctly.
- The Panel noted that a benefit of using Genesys Agent Copilot was that grammar and spelling of summaries would be improved.
- The Panel queried what the standard would be for summaries produced by Genesys Agent Copilot to be uploaded to a claim. The applicant noted that there is already training for what was expected prior to the introduction of Genesys Agent Copilot and that this standard would continue to be expected.
- The Panel queried whether summaries would be used to the train the LLM The applicant confirmed that no ACC data would be used for training.
- The panel noted a concern that Copilot could encourage kaimahi to not use judgment or focus in the same way as they had previously if they knew that a summary would be produced for them. The applicant noted that the introduction of this tool was to aid kaimahi who often had to multi-task and allow them to engage

with kiritaki more. Using Genesys Agent Copilot could lessen the necessity of multitasking and positively impact experience for kiritaki.

- The panel noted that it would be highly valuable to capture data on whether the experience of the call with Agent Copilot improved regarding engagement. The panel suggested investigating whether this could be captured via a survey.
- The Panel queried whether the summary is checked and uploaded at the same time as it is produced or whether it is retrieved from Genesys at a later date. The applicant clarified that straight after each call the kaimahi had a period of time to complete their after-call work and it would be completed at this point.
- The Panel asked for clarification with regard to retention. The applicant clarified that Transcripts and recordings through Genesys are retained for 90 days and the summary produced by Genesys Agent Copilot is retained for 10 days.
- The Panel asked for clarification about the knowledge surfacing and whether Copilot was listening to the call and suggesting links in real time. The applicant confirmed that links would be brought up in real time during the call.
- The Panel queried whether kaimahi would note that the summary was produced, in part, by AI. The applicant noted that this was important to discuss and consider. The Panel also noted that this could be useful in order to compare AI generated summaries against non-AI generated summaries later.
- The Panel queried how the tool worked for speakers other than English. The applicant noted that the tool will summarise what it can, but it may be limited.

Transparency, Engagement and Communication

Transparency is a key part of ACC's Generative AI Models and Services policy (see Appendix 1).

Customers will be informed via the ACC website that certain areas of ACC will use Generative AI to boost efficiency and productivity with the goal of improving client services and experiences, such as reducing call waiting times. This transparency ensures that customers are aware of the role of AI in their service experience.

General public are aware through the government's strategy for a digital public service, service modernisation road map that ACC are using AI on contact centre calls and that this is to be implemented by June 2025 according to the road map.

There will be ongoing engagement with relevant stakeholders about Generative AI's evolving state and how that reflects the acceptable use for organisations like ACC.

The Privacy Impact Assessment (PIA) for Genesys Copilot will be available publicly on the ACC website.

Community consultation and social license

ACC wish to ensure New Zealanders have trust and confidence in the way their data is managed, and the care or services they receive from ACC. This is aligned to the Data Protection and Use Policy (DPUP) principles which are also integrated into ACC's Generative AI Models and Services Policy. The DPUP principles focus on values and behaviours to help ensure personal data practices focus on the wellbeing of people and communities.

The DPUP principle of Kaitiakitanga means that ACC should be acting as a steward of data, in a way that people understand and trust. This principle calls for ACC to be open and transparent about the use of generative AI. As such ACC has updated our generative AI statement on our website and moved this to a more accessible location to ensure customers can find information on our use of AI at ACC.

Overall, the DPUP principles and specifically Kaitiakitanga reinforce the idea that ACC does not own the data they hold, but act as a trusted guardian of that data. Consideration of DPUP principles in this assessment is supplemented by ACC Ethics Panel feedback.

ACC's internal Māori advisors have been consulted regarding risks associated with Māori data, concerns and feedback has been captured in the Ethics Panel feedback. ACC's internal Māori advisors have also agreed to the guidance provided to ACC users to seek assistance if they are unsure of the AI's translation of te reo Māori to ensure accuracy. This is in line with normal process.

Privacy Assessment

The Privacy Act 2020 provide a legal framework that ACC must adhere to. The below table summarises the key considerations of each privacy principle and assesses the compliance of Agent Copilot against each privacy principle

#	Description of Privacy Principle	Summary of personal information involved, use, and process to manage	Assessment of compliance	Link to risk assessment
1	Principle One – Purpose of the collection of personal information Only collect personal information if you really need it.	Principle One requires that ACC carefully considers the purpose for which it collects its information.	We are not increasing collection of information. No new information is being collected in the use of this new tool. No new purpose for collection.	
2	Principle Two – Source of Personal information Get it directly from the people concerned wherever necessary.	Principle 2 requires that ACC collect personal information from the subject of the information where possible.	Source of collection is not changing, in most cases this will be directly from the client, ATA or their provider.	
3	Principle Three – Collections of information from subject Tell them what information you are collecting, what you are going to do with it, whether its voluntary and what the consequences are if they do not provide it.	Principle three requires that there be transparency between ACC and the subject of the information as to why information is being collected, the intended recipients, whether the collection is voluntary or mandatory, and the rights of access and correction.	Subjects are aware information is being collected and used for rehabilitation purposes or related to ACC's functions. However notable risk that the subject is unaware that AI is being used to transcribe and summarise the information they are providing and lack option to opt out. Customers can partially opt out by not having the summary used for their case, but the LLM will still process the information.	R-001 R-002

4	Principle Four - Manner of collection of personal information Be fair and not overly intrusive in how you collect the information	Principle four forbids ACC from collecting information by means that are unlawful, unfair, or unreasonably intrusive.	No change to collection of information.	
5	Principle Five – Storage and security of personal information Take care of it once you have got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	Principle five requires that ACC ensures that personal information is protected against loss, misuse, or unauthorised access by adequate security safeguards.	Genesys copilot has gone through certification and accreditation with the information security team. Information is stored securely and there is limited access to the information.	R-003
6	Principle Six- Access to personal information People can see their personal information if they want to.	Principal six entitles individuals to access their personal information held by ACC.	Calls can be requested within 90-day timeframe. Summary information is held on the claim as per our current retention of 75 year since last use, information is still available for the client to access during the retention period.	R-004
7	Principle Seven – Correction of personal information They can correct it if it is wrong or have a statement of correction attached.	Principle seven entitles individuals to request correction of their personal information held by ACC or have a statement of correction added.	Subjects can request correction of information as per ACC's usual process, no change to this process with the use of this tool though outcome for requests for correction may fall in a grey area, risk noted.	R-005
8	Principle Eight – Accuracy of personal information to be checked before use.	Principle eight requires ACC to ensure that information is accurate and up to date before it is used.	There will be Human oversight with every interaction. Staff members are required to review summaries for accuracy and modify as needed before uploading to system of record.	R-006 R-007 R-008

	Make sure that personal information is correct, relevant, and up to date before you use it.		Accuracy may be an area of risk relating to language, accent, noise etc.	
9	Principle Nine – Not to keep personal information for longer than necessary. Get rid of it once you are done with it.	Principle nine requires that ACC does not retain personal information for longer than is necessary	Calls and transcriptions are kept for 90 days post call Summaries are available for 10 days post call LLM does not retain conversation or summary once data is returned to the staff member Information management have approved these retention periods.	
10	Principle Ten – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies.	Principle ten restricts ACC to using collected information only for the purposes it was collected.	ACC are using the information for the intended reason for collection. To Summarise calls, answer queries and add notes to client files.	
11	Principle Eleven – Limits on disclosure of personal information. Only disclose it if you have a good reason, unless one of the exceptions applies.	Principle eleven restricts the disclosure of personal information. There are several exceptions to this principal including when the disclosure is to the individual concerned or the use is directly related to the purpose for which the information was obtained.	ACC are not disclosing information to third parties.	
12	Principle Twelve- Disclosing information outside New Zealand	Principle twelve restricts the disclosure of personal information outside of New Zealand. Information may only be	ACC are not disclosing information outside of NZ.	

	Only share information with an agency outside New Zealand if the information will be protected.	disclosed if the organisation is subject to the Privacy Act because they do business in New Zealand, will adequately protect the information, or is subject to privacy laws that provide comparable safeguards to the Privacy Act 2020.		
13	Principle Thirteen – Unique Identifiers Only assign unique identifiers where permitted.	Principle thirteen restricts the assignment of unique identifiers. ACC can only assign unique identifiers when it is necessary for its function and cannot assign a particular identifier if another agency has already done so.	Unique identifiers are being processed but not recorded or created by the LLM. Unique identifiers may be in summaries and transcripts as per normal process.	

Assessment of privacy risks and mitigations

The below table describes the risks identified in the privacy assessment in the above table and outlines the implemented and recommended controls to manage those risks.

Any residual risk noted is owned by Service Delivery (Customer Connection) and Technology & Data (Technology & Platforms).

Risk Key - Low: Medium: High:

Ref No.	Description of risk	Consequence for ACC clients or customer	Risk if no controls in place	Existing controls ACC have in place that manage risks identified	Assessment of residual current risk	Recommended additional actions to reduce or mitigate privacy risk	Remaining risk if mitigations are implemented.
R-001	ACC is not transparent about the use of generative artificial intelligences at ACC	ACC customers and clients lose trust in ACC	Major– Possible High	**Information management** • Currently ACC has a statement on its external facing website that outlines the use of Gen AI at ACC. • ACC's use of AI is public on the strategy got a digital public service, service modernisation road map.	**Moderate – possible** **Medium**	Advise callers AI is being used during the call – **The business area will not be pursuing this recommendation, meaning the residual risk is the remaining risk.**	Minor – rare
R-002	Customers are unable to opt	ACC customers	Moderate – possible	**Information management**	Moderate – possible		**Moderate – possible**

	out of their data being processed by artificial intelligence	lose trust in ACC Customers avoid making calls to ACC	Medium	• Customers can partially opt out by advising they do not wish for Copilot to summarise their call, but the call will still be transcribed and processed by the LLM	Medium		**Medium**
R-003	ACC have not got appropriate storage and security practices in place that leads to loss of personal information.	ACC client or customer information is lost, used, or disclosed.	Major - likely High	**Data governance** • ACC will have our own instance for the LLM that sits within our own technical boundaries for Genesys • Data regarding input and output does not move outside technical or geographical boundaries • LLM does not retain the conversation or summary once the data is returned to the staff member. **Information management** • Interactions are stored in ACC's instance of Agent Copilot • Knowledge articles do not contain PII **People** • Staff members will only have access to their own calls **Technology**	Minor – rare Low		**Minor – rare** **Low**

				• Encryption in transit and at rest • Does not have access to web content			
R-004	Customers making an "all information" request are unlikely to be given their transcriptions or summaries held during the retention period	Information is not given to client, potential legislative breach.	Moderate – possible Medium	**Process** • Clients can specifically request these to be provided	Minor – possible Medium	**Process** • Ensure the Client information team are aware these exist and how to obtain these to send out to clients if and when needed. • Ensure frontline teams are aware transcriptions / summaries exist	**Minor – unlikely** **Low**
R-005	ACC cannot determine whether a correction request should be actioned	ACC unsure whether to correct information produced by AI. Potential legislative risk, statement of corrections	Moderate – likely High	**People** • Human review of output **Data governance** • Transcripts are stored for 90 days • Summaries are stored for 10 days	Moderate - possible High		**Moderate - possible** **High**

		unable to be attached					
R-006	ACC uses summary produced by Genesys Copilot that is inaccurate	Decisions made about customers are informed by inaccurate information.	Moderate – possible Medium	**People** • Human review of output **Education** • Education and awareness regarding expectation that each output is checked thoroughly	Minimal – unlikely Low		**Minimal – unlikely** **Low**
R-007	Staff become complacent with use of tool and do not check outputs thoroughly	Decisions made about customers are informed by inaccurate information.	Moderate – possible Medium	**Education** • Education and awareness regarding complacency and expectation that each output is checked thoroughly **Process** • Random CXQ checks each staff member has at least two calls checked each month.	Minor – unlikely Low		**Minor – unlikely** **Low**

R-008	Information produced by Genesys Copilot is not accurate to the conversation when translating language e.g. Te reo Māori.	Inaccuracies may change the context of a conversation and/ or influence decisions about customers	Moderate – possible Medium	**People** • Human review of output **Education** • Education and awareness regarding translations **Process** • User is able to submit for a peer review to ensure the summary is accurate if they are unsure **Technology** • Additional words can be added to the Genesys dictionary	Minor – unlikely Low	**Data governance** • Monitor translations during roll out to inform future improvements or additions to dictionary	**Minimal – Unlikely** **Low**
R-009	US Cloud storage act the US can request information held in AWS	Information processed by the LLM may have to be disclosed to the US	Moderate – unlikely Medium	**Data governance** • Transcripts are only stored for 90 days • Summaries are only stored for 10 days	Moderate - rare Low		**Moderate - rare** **Low**
R-010	Knowledge articles are out of date / not updated	Incorrect information may be passed onto a customer	Minor – Unlikely Low	**People** • Human review of knowledge **Information management** • Knowledge to be kept up to date manually by CSAs	Minimal - Unlikely Low		**Minimal - Unlikely** **Low**

R-011	Conflicting information in knowledge articles	Incorrect information may be passed onto a customer	Minor – Unlikely Low	**People** • Human review of knowledge	Minimal - Unlikely Low		**Minimal Unlikely** **Low**
R-012	The Vault servicing frontline staff though process and policies are different.	Staff using processes or policies that do not align with best practice	Minor – Unlikely Low	**People** • Human review of knowledge **Technology** • Ability to click through to knowledge source	Minor – Unlikely Low	**Information management** • Additional knowledge to be entered when onboarding frontline staff • Information to be checked at regular intervals	**Minimal Unlikely** **Low**

Risk matrix – *Use your likelihood and consequence to determine your risk rating*

		Consequence				
		Minimal	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	Medium	High	High	Very High	Very High
	Likely	Medium	Medium	High	High	Very High
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	High

Risk escalation – *Use your risk rating to determine what action you need to take*

Residual Risk Rating	What does it mean?	What needs to be done?	Who can accept?
Very High	Immediate and imperative failures. Significant risk to the achievement of goals and objectives.	Urgent and active management required, including treatment plan and immediate escalation.	Chief Executive
High	Major events. A risk that can interrupt what we are trying to achieve. High risk to business objectives.	Active management and regular review, including establishing a treatment plan to enhance controls.	Deputy Chief Executive (DCE)
Medium	Delivery, operating and compliance risks that interfere with what we are doing. Moderate risk to business objectives	Monitor and review. A treatment plan should be established based on review of existing controls.	Head of Manager (Tier 3)
Low	Minor or insignificant occurrence. Low risk to business objectives.	Normal controls and monitoring measures.	Tier 4 Manager

Action Plan

There are some ongoing actions to monitor using Genesys Copilot at ACC. The below table specifies the necessary actions, who is responsible for those actions, and the timeframe for completing the action.

Agreed Action	Who is responsible	Timeframe
Advise Privacy if there is any change to privacy risk and controls	Product owner	Continuous
Monitor changes or updates to Agent Copilot by Genesys.	Product owner	Continuous
Update PIA if scope changes or information is out of date	Product owner	Continuous
Investigate monitor and advise Privacy of any major incidents that are contributed to by Agent Copilot	Product owner	Continuous
Continue education for newly onboarded users	Product owner	Continuous

Ethics risk assessment

Number	Description of ethical risk	Control in place	Suggestion
1	ACC is not transparent with kiritaki about how their information is being processed, this goes against ACC's Gen AI policy and the algorithm charter.	ACC has a generative AI statement on our external facing website	Consider changing the statement at the start of a call - **The business area will not be pursuing this recommendation**
2	There is no informed consent from kiritaki meaning they may be unaware their information is being processed by AI and have not agreed to this.	ACC has a generative AI statement on our external facing website	Consider changing the statement at the start of a call - **The business area will not be pursuing this recommendation**
3	Kiritaki are unable to opt out of their information being processed by AI as there is no ability to turn off this functionality.	Part opt out available where information will still be processed by Genesys copilot, but the summary will not be used, the staff member will create their own	
3	Genesys Copilot could encourage kaimahi not to use judgement or focus in the same way knowing a summary would be produced for them.	Agent Copilot risk awareness will be incorporated within the toolset training for staff, to ensure inadvertent bias and discrimination from auto summaries are recognised and handled by a human	
4	Summaries may be incorrect or inaccurate when a kiritaki speaks another language e.g. Te reo Māori.	Human oversight of all interactions. Kaimahi can ask for support with additional reviews through current support mechanisms. Translation services available as per current processes	

		Dictionary can be update with commonly used words or mistranslated words.	

Risks

The main privacy risks are relating to inaccurate information being produced by Genesys Copilot in transcriptions and summaries. These risks could lead to breaches to the information privacy principles of the Privacy Act 2020 including correction (IPP7) and accuracy (IPP8). Further concerns were also noted for collection of information (IPP3) and access to information (IPP6).

The risks relating to correction and accuracy of information are somewhat alleviated by human oversight. This will be a key element to ensuring that summaries are accurate and edited appropriately before being stored in the system of record. Education and training will be provided prior to the use of the tool and existing monthly monitoring of calls and contacts will continue to support staff in maintaining summary standards. Education and training offered before use of Genesys copilot agent includes how the tool works, how to review summaries and include what is expected of staff members and getting support.

Risk arising in the case of a customer wanting to 'correct' a partially AI generated contact is likely to be ongoing as once the call is no longer retained (90 days) there will be no call to compare notes to, this is a current risk in our system but likely to be increased by AI use. This is compounded by the inability to add statement of corrections to our contact notes.

Concerns relating to collection of information have been mitigated by providing a more comprehensive generative AI statement on ACC's public facing website which is now more accessible to customers looking for this information. Suggestion from the Ethics panel was to include a statement on the phone line to advice of the use of AI, this was also a recommendation during the privacy risk assessment, the business has decided against implementing this at this stage.
There is still a notable concern here regarding transparency as general customers who have not read our Generative AI statement on the website will be unaware AI is being used to process their information and will be unable to request a partial opt out or contact us in another way if they are unaware of its use. Transparency is a key point in many of our AI guidelines e.g. Algorithms charter, Public service AI framework, Data protection and use policy and ACC's own Generative Artificial Intelligence policy

Risks relating to access will be mitigated by ensuring training for our client information team, complaints team and frontline staff members.

Benefits

Agent Copilot is expected to provide the following value and benefits to the Contact Centre and other frontline Recovery teams:

- Reduction in overall Average Handle Time (AHT) across Contact Centre and Recovery teams as our staff members will be augmented with assistive AI capability:
    - Expected reduction of ~1-minute AHT for frontline staff through the advanced call summarization.
    - Expected reduction of ~30 seconds AHT per interaction within Contact Centre as they handle shorter interactions overall & are already quite mature in their ability to process After Call Work.
    - The reduction in AHT will mean that customers' queries and issues are resolved faster.
- Reducing '0800 number' expenditure will improve the IT operating budget by decreasing client hold times. This reduction in average handle time (AHT) will enhance business efficiency and improve customer experience through quicker query resolution and reduced frustration.
- Reduced cognitive load for both Contact Centre and other Recovery staff as less note taking will be necessary during the interaction. Staff members can focus more on the conversation, providing more attentive and personalised service to customers.
- We expect to see a reduction of internal call transfers and consults from the contact centre through to our Practice Mentors and CSAs as Agent Copilot will be delivering consistent knowledge material contextualized to the conversations to our staff members. This will speed up new starters' competency in the Contact Centre, requiring less upfront training to handle real customer interactions. In turn, clients will interact with knowledgeable and skilled staff members sooner, leading to a more consistent and high-quality service experience.

Conclusion and recommendation

The main privacy risks relate to correction (IPP7) and Accuracy of information (IPP8). Further concerns relate to collection of information (IPP3) and access (IPP6). There are multiple technical and non-technical controls that mitigate against severe privacy risk.

ACC Privacy team have recommended the following actions be taken to ensure that risks are continuously controlled with the use of Genesys Copilot.

- Staff members using the tool will be responsible for ensuring outputs produced are accurate before being moved to the system of record. All users will complete training regarding the important of checking summaries for accuracy.
- Risk awareness will be incorporated within the toolset training for staff, to ensure inadvertent bias and discrimination from auto summaries are recognised and handled by a human (Staff member) during the editing of summary notes.
- In cases that use cases expand the product owner or representative will liaise with ACC Privacy team to ensure that no new privacy concerns arise because of a new use.
- If there are changes to Genesys Copilot in ways that may impact privacy, the product owner or representative will liaise with the Privacy team to review the PIA and ensure that controls are in place to mitigate any additional risk
- An assessment will be necessary from Information and Security and Privacy at ACC if it were proposed that web content is turned on.
- ACC is transparent with its customers that it will use AI that processes customer data.
- Transcriptions and recordings are deleted after 90 days. If there is a correction request that doubts the accuracy of an AI summary after 90 days, there is currently no further record to check against if staff do not have a clear recollection of the call. Recommend considering how correction requests would be considered outside this 90-day timeframe.
- Knowledge is checked and updated in the Genesys system periodically

References and resources

References

Privacy policy | Genesys

Genesys Cloud Services terms and conditions - Genesys Cloud Resource Centre

Ethics and Compliance | Genesys

Genesys Agent Co-pilot FAQ

Understand Agent Copilot AI models and LLM input - Genesys Cloud Resource Centre

Data Protection and Use Policy (DPUP) | NZ Digital government

Algorithm charter for Aotearoa New Zealand - data.govt.nz

Algorithm-Charter-2020_Final-English-1.pdf

Public Service AI Framework | NZ Digital government

Service Modernisation Roadmap | NZ Digital government

ACC References and resources ACC References and resources

ACC Generative Artificial Intelligence policy

Generative AI Models and Services Policy Guidelines

AI Controls Framework Comms.pptx

Risk Management Reference Guide and Matrix.pdf

Generative Artificial Intelligence (Gen AI)

Appendix 1 ACC Generative Artificial Intelligence Policy

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.

Policy Statements:

1. **We are transparent about all Generative AI usage.**
   ACC staff are transparent about the use of Generative AI Models and Services including any potential limitations or biases.

2. **We always have human oversight throughout the use of Generative AI Models or Services**
   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. **We will make data security and privacy paramount in the design and use of Generative AI** Models and Services
   All Generative AI Models and Services must be designed, developed, and used with privacy and security in mind. Appropriate security controls and measures must be implemented to protect against cyber threats and any unauthorised access to or sharing of information.

   All new instances of AI technology, as well as any new feature or use cases for existing AI systems, must follow standard approvals and governance processes. This includes obtaining the necessary clearances through the Certification and Accreditation process and securing approval from the Change Advisory Board or Solution Alignment Board (as applicable) before any deployment can proceed.

4. **We 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.

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, and data is protected through appropriate data privacy and security safeguards.

6. **We will apply an ethical lens to all Generative AI Models and Services use**
   All large scale (or 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 consider and take reasonable steps to protect and respect ACC and third-party intellectual property rights.**
   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.

   ACC staff must 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
   ▪ 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, cannot be assured.

8. **When an incident or breach occurs, we fix it and learn from it**
   When an issue occurs, we fix it and learn from it. We do this in a transparent and constructive way and seek longer term solutions that help prevent similar events from occurring in the future.

Appendix 2 – ACC's Generative AI Controls that relate to Genesys Copilot

Control title	Control description	Control Operator
Awareness of AI specific legal and regulatory requirements	The control operator maintains awareness of industry, technical and applicable legislative / regulatory requirements to ensure that ACC's strategic direction is in line with these requirements and changes. Any changes and potential impacts will be raised at the Information Governance Group (IGG) for further consideration and potential action. It is also the responsibility of the IGG to ensure members of the AI Working Group (AIWG) are made aware of any changes	Charmaine Bowring
Genesys Copilot Privacy Impact Assessment	As required on an ongoing basis the Control Operator will review and verify that Privacy AI impact assessment activities are appropriate to: - evaluate the potential negative impact of a system - how quickly a system changes, - and that assessments are applied on a regular basis Where needed the Control Operator will align organisational impact assessment activities with relevant regulatory or legal requirements.	Reinette Woollands
Genesys Copilot Product Review	As required or an ongoing bases, the Control Operator will conduct review of Genesys Copilot. This will include: - Alignment with organisational objectives and regulations, - Identification of potential improvements -Any applicable findings are presented to the IGG . *An evaluation of the effectiveness of existing controls New features roll out and impacts are assessment	Reinette Woollands
AI System & Services Inventory	On a quarterly basis, the Control Operator will review and validate the mechanisms in place for inventorying AI systems and the inventory itself, ensuring that they are: Comprehensive and accurate Aligned with risk mitigation needs Effectively managed in accordance with the ACC's risk approach and priorities Necessary adjustments will be made in response to changes in risk priorities, system additions, and/or other internal/external needs.	Dane Howarth

AI Risk Management Roles and Responsibilities (Enterprise Wide)	On a quarterly basis attestations are completed by People leaders across the organisation affirming understanding to - the defined roles and responsibilities for AI risk management in internal contexts. - check the methods used for communication of roles and responsibilities as defined in the AI policies across ACC and verify understanding through assessments.	Nicholas Tuohy
AI Management Policy	On an ongoing basis, the Control Operator will monitor and incorporate guidelines and best practices for trustworthy AI within ACC's current policies, procedures, and training materials, ensuring ethical and transparent operations. Any required changes will be escalated to the IGG for consideration.	Kerry Southee
Certification and Accreditation	Every 2 months the Chief Information Security Officer (CISO) certifies the new Certification and Accreditations for solutions, to confirm they are within risk appetite, and the Chief Technology and Innovation Officer (CTIO) accredits them to operate. The Certification Confirmation process covers all new solutions (prior to release in production) as well as existing solutions that have not had a review in 3 years. All information is stored in a secure location.	Matthew Rounthwaite
Staff Awareness & Training	Every Business Unit's Control Operator conducts monthly assessments to verify ACC staff's understanding of AI roles and responsibilities through the reviewing of training records and documentation to ensure that appropriate training and supporting awareness programmes are in place as outlined in ACC's AI Policies.	SERVICE DELIVERY – ROSS STERLING
Genesys Copilot System MAINTAINANCE	On an ad-hoc basis, when new features are introduced the Control Operator will verify the appropriateness and effectiveness of the testing process of Genesys Copilot by reviewing the outcomes of testing that has taken place. Where identified, the testing process will be realigned and/or guidelines for testing will be further reviewed.	Reinette Woollands
Genesys Copilot Stakeholder Engagement Process	On an annual basis the Control Operator will review the effectiveness of the AI stakeholder process by selecting a sample of stakeholder engagements that took place over the past 12-months, comparing them to both the processes outlined in ACC's AI Policies and the outcomes of the engagements.	Reinette Woollands
Genesys Copilot stakeholder & User feedback	On an annual basis the Control Operator will review and verify that stakeholder and user feedback is considered and appropriately addressed as outlined in ACC's AI Policies	Reinette Woollands