ACC Privacy Impact Assessment (PIA)

Microsoft 365 Copilot

February 2024

Contents

Overview

This privacy impact assessment (PIA) evaluates the privacy implications and risks of Accident Compensation Corporation using Microsoft 365 (M365) Copilot, an AI-powered assistant that helps users with various work tasks. It will cover the following aspects:

- The purpose and scope of the project, and the objectives for using Microsoft 365 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 Microsoft 365 Copilot, including General Data Protection Regulation (GDPR) and other international privacy legislation.
- Privacy and Generative AI policies and guidelines that will be applied to the use of Microsoft 365 Copilot at ACC.
- The data collection and processing activities that will be performed by Microsoft 365 Copilot, and the types and sources of personal and sensitive health information that will be involved.
- The ethical concerns associated with using Microsoft 365 Copilot at ACC.
- The privacy risks and challenges that may arise from using Microsoft 365 Copilot at ACC, and the actions and measures that will be taken to prevent and contain privacy risk.
- The benefits evaluation of implementing M365 Copilot at ACC, and the evidence and examples of how it can enhance productivity, creativity, skills, collaboration, knowledge, and work experience across ACC.
- The conclusion and recommendations for using Microsoft 365 Copilot at ACC, and the areas for improvement and further discussion.

The PIA is based on the information and guidance provided by ACC, Microsoft, 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

Generative AI and M365 Copilot

This PIA focuses on the use of Microsoft365 Copilot (M365 Copilot), a generative artificial intelligence, within Accident Compensation Corporation (ACC). Generative artificial intelligences are tools used to generate content such as code, text, and images. Generative AI often utilise Large Language Models (LLMs) which contain a wealth of data. Generative AI applications like M365 Copilot work by taking a prompt, matching them to patterns in training data, and then piece by piece they use probability to predict what should come next in a sequence until the task is fulfilled. If utilised well these applications can make completing tasks more efficient, therefore increasing productivity levels and reducing costs.

M365 Copilot is an application used within the suite of Microsoft products. It is a productivity tool that utilises large language models to generate content across Microsoft365 apps such as Word, Excel, Teams, and PowerPoint. It can be used to summarise documents, produce a PowerPoint, and summarise meetings. Microsoft's intention is for it to support users in the context of their own work across the apps that they use (Appendix Four details the Microsoft that are encompassed by M365 Copilot).

ACC and M365 Copilot

Microsoft products are used extensively at ACC with high levels of adoption across the full product set. ACC already uses SharePoint (and have a SharePoint-based intranet), OneDrive, Microsoft Teams, Exchange Online, the full Microsoft 365 Office Suite and several applications in the new Viva Employee Experience suite. ACC use Entra ID (formerly Azure Active Directory) and have implemented Azure Information Protection.

In September 2023, Microsoft offered ACC the opportunity to take part in a paid 'Early Access Program' for Microsoft 365 Copilot, including licenses for 300 users and direct access to Microsoft specialists to support our implementation and use of Microsoft 365 Copilot. Microsoft 365 Copilot integrates into several of the Microsoft 365 applications to allow users to leverage artificial intelligence functionality. It also has a chat feature within Microsoft Teams that allows users to find and ask questions about content from across our internal repositories and uses intelligence from a Large Language Model (LLM) to form the response/output.

ACC have identified several general use cases for Microsoft 365 Copilot that have been explored in a phased pilot within the early access program, after which a decision will be made whether, and how widely, to make Microsoft 365 Copilot available across ACC.

There have been seven use cases that were identified for a Microsoft 365 Copilot pilot trial in the ACC context. Each of these use cases offer multiple points of value. These use cases include:

1. *Recapturing and summarising meetings.*
   Value:
   a. Reduction in time for people who usually take meeting minutes.
   b. Reduction in time and effort for meeting attendees by providing the ability to revisit the main points of a meeting and easily access action items.
   c. Improved quality of meeting discussions by offering attendees the ability to get ideas for discussion prompts/questions.

    d. Improved access to information by allowing those who were invited but could not attend access a summary of key points.
2. *Summarising documents and email threads.*
    Value:
    a. Reduction of time and effort.
3. *Drafting documents, presentations, emails, and forms.*
    Value:
    a. enhanced content quality.
    b. reduction in time and effort for content production.
    c. aiding people who have neurodiversity or accessibility needs.
4. *Generating ideas for non-client-facing functions e.g. ideas for improving productivity in a back-office team.*
    Value:
    a. Enhanced ideation quality and reduction in time.
5. *Data processing and reporting.*
    Value:
    a. improved reporting and processing outputs (including for people who aren't familiar with complex Excel functionality/formulas).
    b. reduction in time and effort.
6. *Generating draft SharePoint pages e.g. creating education pages or FAQs.*
    Value:
    a. enhanced content generation.
    b. reduction in time and effort.
7. *Information discovery – using M365 Copilot chat to find internal information such as email content or file references.*
    Value:
    a. Improved speed to delivery from being able to quickly pull information from multiple sources.
    b. Reduction in time and effort.

The pilot has given ACC the ability to assess Microsoft 365 Copilot's impact on data security, privacy, and compliance and gather feedback from pilot participants, including benefits of using Microsoft 365 Copilot to create efficiencies and improve productivity and user experience. ACC wishes to take a cautious and considered approach to this technology and have applied mitigations to ensure the use of Microsoft 365 Copilot does not pose a risk to client service delivery or data, security, and privacy compliance. This includes applying ACC's new Generative AI Models and Services policy and guidelines and working closely with Privacy and Information Security Teams at ACC.

The use of artificial intelligence tools to improve user experience and productivity aligns with ACC's 'Ki te ao mārama' guiding principle - to grow and evolve, and ACC's strategic objective to 'enhance people systems capability'. As early previewers of Microsoft 365 Copilot, ACC will share its approach and outcomes with interested stakeholders from other New Zealand Government Departments, including the Department of Internal Affairs. This is not ACC's first use of generative artificial intelligence. Github's Copilot, powered by GPT-4 is already used at ACC to generate code. It does not use personal information and has access limitations applied to it. To date it has offered time and cost savings and there have been no adverse findings from its use. Future uses of generative AI are also being considered such as Microsoft Copilot for Power Automate and Copilot for Viva Engage.

Scope and current/future state

The scope of this document covers the widespread use of Microsoft 365 Copilot at ACC – but the approach to its deployment has been phased which has allowed ACC to formulate controls to mitigate any privacy risk before rolling it out wider across the organisation.

The purpose of completing a PIA is to identify the impact that using Microsoft365 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.

Testing and initial product feedback

An initial cohort of 25 users have tested Microsoft 365 Copilot's functionality, controls, and adherence to permissions. The testing confirmed that Microsoft 365 Copilot honours existing user permissions and did not uncover any major issues regarding privacy and security controls. There were some tests that brought back unexpected results – mostly to do with functional limitations and issues/bugs - but nothing that prevents ACC from moving forward with use case discovery.

Testers were asked to provide on their overall experience using M365 Copilot. The consensus was that M365 Copilot has some useful features that will help with productivity and work quality. But it also returned quite a lot of strange/inaccurate results and errors. Some of these are due to users requiring additional training in the best way to use/prompt M365 Copilot, while others were due to the product simply being new and immature. Testers reiterated the need for human review/oversight of results.

The information discovered helped the M365 Copilot team to revise its terms of use and the guidance given to users – e.g. how to write effective prompts and to always apply human oversight/review to outputs (including those involving formal Te Reo Māori translation).

Phased approach to proof of value pilot

The next stage has involved people from a cross-section of ACC functions identifying and validating use cases and possible business benefits and providing product feedback. 50 users started this during February 2024, an additional 180 users at the start of March 2024 and up to 45 more during the months following that through until October 2024 (up to a maximum of 300 users). As of May 2024, there were 291 users. Throughout this phase there have been no instances of users being able to access content they did not have permission to view. There have been a couple of instances where users discovered that they had permissions to view documents that they should not have, and these instances have now been rectified. This should not prevent ACC from moving forward with the use of M365 Copilot and controls are in place to review permission controls.

Use after the pilot

A decision regarding the ongoing use of Microsoft 365 Copilot at ACC will be made based on the outcomes and feedback from the pilot phase. This PIA applies to a set of defined use cases. If, in the future, it is decided to extend the scope of approved use cases, further privacy assessment will need be carried out.

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 Microsoft 365 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 Microsoft 365 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 Microsoft 365 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. Although Microsoft is located within the jurisdiction of this act, it is not relevant to this PIA as Microsoft 365 Copilot does not 'store data'.

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 (which Microsoft does). Meeting these regulations would be an obligation on Microsoft, but ACC would need to review any impact the regulations have on the functionality or risk profile of Microsoft 365 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 Microsoft 365 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 Microsoft 365 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.

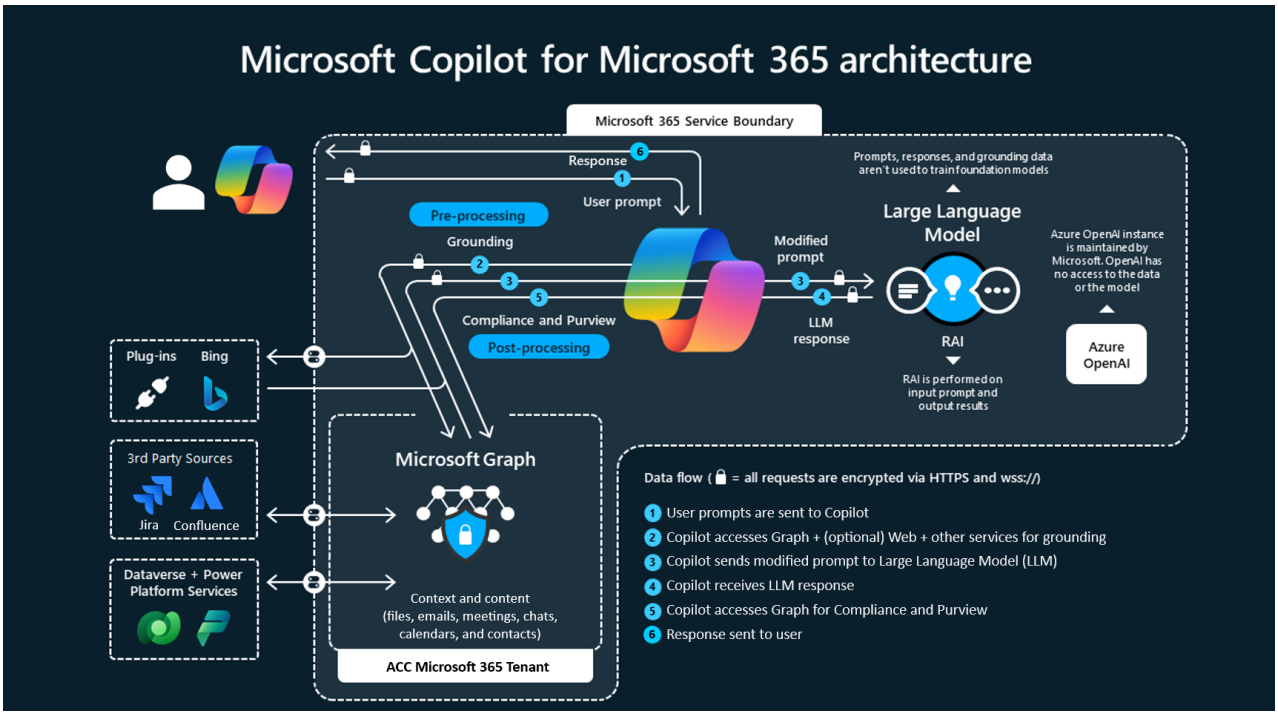
ACC have complied with all these expectations.

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. Transparency is at the forefront of any Generative AI usage.
2. ACC will have human oversight included throughout the use of any Generative AI model.
3. Data privacy and security are paramount.
4. ACC will actively protect Mātauranga Māori, tikanga, and taonga (Māori Protected Materials).
5. ACC will comply with all applicable laws and associated policies.
6. All Generative AI Models and Services must have a focus on ethical use.
7. We will collaborate with relevant stakeholders when considering or using Generative AI Models and Services.
8. Clarity on usage purposes.
9. We will consider and take reasonable steps to protect and respect ACC and third-party intellectual property rights.
10. We will always follow guidelines.

How Microsoft 365 Copilot works



1. M365 Copilot receives an input prompt from a user in an app, such as Word or PowerPoint or from the M365 Copilot chatbot in Teams.

2. M365 Copilot then pre-processes the input prompt through an approach called grounding, which improves the specificity of the prompt, to help you get answers that are relevant and actionable to your specific task. The prompt can include text from input files or other content discovered by M365 Copilot (e.g. SharePoint and OneDrive files, emails, meeting transcripts, chats, calendars and contacts and 3rd party sources ACC have made available to the Microsoft Graph search such as Jira and Confluence content).

3. M365 Copilot sends this prompt to the LLM for processing. M365 Copilot only accesses data that the individual user has existing access based on their existing Microsoft 365 role-based access controls.

4. M365 Copilot receives a response from the LLM.

5. M365 Copilot takes the response from the LLM and post-processes it. This post-processing includes other grounding calls to Microsoft Graph, responsible AI checks, security, compliance and privacy reviews, and command generation.

6. M365 Copilot returns a response to the app, where the user can review the response.

Technologies are utilised to encrypt customer content both at rest and in transit as described in the next section of this document.

Microsoft 365 Copilot: Data collection and processing

Microsoft 365 Copilot is an AI-powered assistant that helps users with various work tasks, such as writing, editing, formatting, researching, presenting, designing, coding, and more. Microsoft 365 Copilot uses natural language processing and its own Large Language Model (LLM) to understand the user's intent, context, and preferences, and to provide relevant suggestions, feedback, and assistance.

One feature that can be turned on or off by the product owner is Microsoft Copilot's ability to interact with web content. If turned on, based on the user's prompt, Copilot for Microsoft 365 can determine whether it needs to use Bing to query web content to help provide a relevant response to the user. If this is needed, the query is passed to the Bing Search API, which is part of the Bing Search service, to retrieve information from the web to ground a response.

Once web data is received, Copilot for Microsoft 365 passes the web data to the LLM to generate a richer response by including the latest information from the web and any relevant citations. In this process, the user's prompts and Copilot's responses remain within the Microsoft 365 service boundary. Microsoft Copilot 365 would abstract the information requiring a web search from the user's prompt and then only this web search query would go to Bing Search API outside the boundary. Queries sent to the Bing Search API by Copilot for Microsoft 365 are disassociated from the user ID or tenant ID. Web search queries might not contain all the words from a user's prompt. They are generally based off a few terms used to find relevant information on the web. There are controls available to manage the use of web content for both admins and users. Currently ACC has the web content feature for Copilot turned off. If it were to be turned on this would require review from ACC Information Security and Privacy teams.

Microsoft 365 Copilot can be accessed through various Microsoft 365 applications, such as Word, Excel, PowerPoint, Outlook, Teams, and OneNote (see Appendix Four). To provide its services, Microsoft 365 Copilot needs to, at times, collect and process some personal information from the users and their work documents. The types and sources of this information may include:

- User identity and profile information, such as name, email address, phone number, job title, department, and organisation
- User preferences and settings, such as language, region, time zone, and accessibility options
- User feedback and ratings, such as comments, suggestions, and ratings on the quality and usefulness of Microsoft 365 Copilot's services
- User activity and usage data, such as the frequency, duration, and type of Microsoft 365 Copilot's services used, the commands and queries issued, the suggestions and feedback received, and the actions and outcomes taken.
- User work documents and content, such as the text, images, tables, charts, graphs, and other elements in the documents created, edited, or viewed by the user, and the metadata associated with them, such as the file name, size, format, location, and version.

How does M365 Copilot protect ACC customer data?

Individual prompts, responses, and ACC data accessed when using Microsoft 365 Copilot aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot. This means there is no risk that any input of ACC data into the LLM will show up in responses to other users. The training boundaries across Microsoft 365 Copilot's LLM mitigate any risk of exposure to ACC client personal information.

Microsoft 365 Copilot does not integrate into ACC's authoritative client record systems that host client, claim and health information, such as EOS and Salesforce. Therefore, there is no privacy risk with Copilot being able to access and collect information from within those systems and use it as a source for its outputs. Terms of use also requires that users do not directly input personal information into M365 Copilot.

Technologies are utilised to encrypt customer content both at rest and in transit, ensuring strong security measures. Connections are safeguarded using Transport Layer Security (TLS). The transmission to Azure OpenAI Service is facilitated through the Microsoft network to ensure the reliability and safety of the transfer.[1]

Data stored about user interactions with Microsoft Copilot

When a user interacts with Microsoft 365 Copilot apps, Microsoft store data about these interactions only within ACC's tenancy. The stored data includes the user's prompt, how Copilot responded, and information used to ground Copilot's response.

For example, this stored data provides users with Copilot interaction history in Microsoft Graph-grounded and meetings in Microsoft Teams.[2] This data is processed and stored in alignment to contractual commitments with Accident Compensation Corporation, other content in Microsoft 365, and is discoverable for audit purposes.

The data is encrypted while it's stored and isn't used to train foundation LLMs, including those used by Microsoft 365 Copilot. To view and manage this stored data, admins users can use Content search or Microsoft Purview. Admins can also use Microsoft Purview to set retention policies for the data related to chat interactions with Copilot.

Data deletion with Co Pilot

To delete a user's history of interactions with Microsoft 365 Copilot, which includes user prompts and the responses returned, Microsoft 365 admins can submit an online support ticket in the Microsoft 365 admin centre. In this ticket, admins should include the Tenant ID and the users Object ID for which they want data deleted. The ticket will mark the history for permanent, hard deletion.[3]

---

[1] Microsoft. "Encryption in the Microsoft Cloud". Microsoft Learn. August 9, 2023. https://learn.microsoft.com/en-us/purview/office-365-encryption-in-the-microsoft-cloud-overview. Accessed January 26, 2024.

[2] Microsoft. ''Get started with Microsoft 365 Chat''. Microsoft Copilot. https://support.microsoft.com/en-gb/topic/get-started-with-microsoft-365-chat-5b00a52d-7296-48ee-b938-b95b7209f737. Accessed January 28, 2024.

[3] Microsoft. ''Deleting personal data''. Microsoft Learn, 23rd May 2023. https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365#deleting-personal-data. Accessed January 25, 2024.

Offshore data and data transfer

Microsoft 365 Copilot requests are routed to the LLM in the closest regional data centre (for ACC this is in Australia), but they can also be processed in other regions (including US and EU) where capacity is available during high utilisation periods.[4] Copilot for Microsoft 365 adheres to the compliant boundaries that ACC have already agreed to in their terms of service with Microsoft. All data in transfer will be encrypted. There is no data stored by Microsoft– any outputs from Microsoft 365 Copilot will reside in ACC's Microsoft 365 applications in the usual agreed storage repositories (in the closest regional data centre).

[4] Microsoft. Data, Privacy and Security for Microsoft Copilot for Microsoft 365. Microsoft Learn, 23rd January 2024. https://learn.microsoft.com/en-us/microsoft-365-copilot/microsoft-365-copilot-privacy. Accessed January 26, 2024.

How does ACC protect client and staff personal information across Copilot use?

To mitigate privacy risks ACC has limited the ways in which Microsoft 365 Copilot can be used whilst completing the proof of value pilot. M365 Copilot has been limited to use within the Microsoft products ACC has approved and uses. ACC has also ensured that Microsoft Copilot has no access to ACC client record systems which contain most of ACC's client personal information.

Whilst the Terms of Use and Generative AI Service Policy restrict personal information from being explicitly inputted into the tool, there are still documents within ACC's Microsoft products containing personal information could be used as an input or that could be retrieved by the tool. This means that it is foreseeable that outputs could end up containing personal information despite not having used it as a direct input if the user has access permissions to documents that contain personal information. To limit risk, good data governance is of critical importance. Copilot will only be able to access the documents that the user utilising M365 Copilot has access to across ACC's Microsoft products. Accuracy checking and human oversight will also feature in the tool's use to ensure that outputs produced by the tool are free of errors. Security classification labels which at ACC include client in-confidence, staff in-confidence, commercial in-confidence (and others) will transfer from the documents used as an input to documents produced as outputs alerting the user that the produced document contains information that contains personal or commercial information, for example. This is not a technical block, but a control for alerting the user as to the information contained in the document may be of a sensitive nature and should be reviewed with that in mind.

Both technical and non-technical controls have been put in place to ensure that the Information Privacy Principles (IPPs) are adhered to whilst utilising M365 Copilot at ACC.

ACC technical privacy controls

ACC has implemented several technical controls to help protect its data and apply permissions to files to ensure only the right people have access to them. This includes having:

- files and intranet content in SharePoint with inbuilt permission controls,
- processes in place to manage Microsoft 365 Group creation, membership, and permissions,
- data classification labelling,
- Entra ID access authorization, multi-factor authentication, and role-based controls,
- Azure Information Protection,
- Microsoft Purview Data Loss Prevention,
- Microsoft Defender.

These controls will be vital for ensuring that Microsoft 365 Copilot will only show ACC people information that they have the requisite permissions to view, whilst protecting information from inappropriate access from other internal staff and external parties.

Managing access to Microsoft 365 Copilot

ACC's approach to onboarding staff to use Microsoft 365 copilot is stringent.

Access to the Microsoft 365 Copilot license is controlled by Microsoft Entra Group membership and Microsoft Teams Policy. Pilot participants must submit a form to agree to the 'Terms of Use' (see Appendix 2), then a Teams Power Automate flow triggers an approval process. One of two 'Group' administrators checks they match on the list of agreed participants (as approved by the

ACC Microsoft 365 Product Owner), and then approves the request. Power Automate will add the requestor to the license group which enables Microsoft 365 Copilot functionality within the various Office applications (Word, Outlook, PowerPoint etc.) A Microsoft Teams administrator then adds the participant to a Microsoft Teams Policy which provisions them with the Microsoft 365 Copilot chat functionality within Microsoft Teams.

Copilot access to web content.

ACC has currently turned off web content for Microsoft 365 Copilot. This means that no data that has been input into Microsoft365 copilot will be sent to Bing Search API. This mitigates the risk of input data remaining outside of ACC's tenancy. If there were a change made to Copilot's access to web content this would require a further risk assessment to be completed by ACC's information security and privacy teams.

ACC non-technical privacy controls

There are privacy controls ACC has implemented, outside of technical guardrails, that will mitigate ongoing privacy risks attributed to M365 Copilot. These include:

Education and training

ACC will provide training and resources to assist users of M365 Copilot (see Appendix 3). This training will enable users to understand the risks associated with using M365 Copilot, the terms of use they need to apply to mitigate these risks, and best practices for responsible AI use – including not including confidential or sensitive information in prompts, and the need to review any outputs before using or sharing them. They will also be asked to familiarise themselves with, and abide by, ACC's Generative AI Models and Services Policy and Guidelines. Microsoft 365 Copilot user resources and training will be regularly reviewed and updated to ensure they meet current guidelines and best practices.

ACC have an ongoing programme to educate all staff on best practices regarding file management, sharing and permissions to mitigate risks associated with incorrect access permissions. This takes the form of live online training sessions, pre-recorded videos, and guidance published via ACC's intranet pages and intranet news stories.

There will need to be increased investment in education as the number of individuals utilizing M365 Copilot increases.

Human oversight

M365 Copilot can be used to complete a wide range of tasks. This includes, but is not limited to, summarising meetings, production of PowerPoints based off other documents, and answering questions about data in excel. If these outputs are to be used by ACC, it is important to know the M365 Copilot outputs are accurate. If inaccurate outputs containing personal information are used by ACC, this poses a risk to the privacy principle of accuracy (IPP8) Human oversight is required as part of ACC's Generative AI models and Services Policy (see Appendix 1). Human oversight will be a key feature of monitoring Copilot use across ACC. Analysis of this control is included in the risk and mitigation table. Users undergo training on ways to review information produced by M365 copilot and outlines expectations of thorough review.

Applying relevant policies and guidelines

ACC will apply relevant policies and guidelines as outlined in pages 7-9 of this document. Adherence to these policies will be monitored and governed by both the ACC Microsoft 365 Product Owner and the ACC Generative AI Advisory Panel.

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. The 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 Microsoft 365 copilot will provide input to ACC's six-monthly AI Risk Management Process Review and annual AI Stakeholder Engagement Process review.

They will also reassess Microsoft 365 Copilot and user guidelines and training if the ACC Generative AI Governance Group make changes to ACC's approach to Generative AI based on legislative or regulatory changes.

See Appendix 3 for a table of ACC's Generative AI risk controls that relate to Microsoft 365 Copilot, and information on how these will be addressed.

Ethical concerns

ACC's internal ethics panel considered the use of Microsoft 365 Copilot at ACC. They raised the following concerns/observations but were satisfied with how these risks have been addressed and were supportive of the proposed trial to identify possible business benefits for its use at ACC.

- The panel noted that there was a risk that users would not recognise the importance of reviewing outputs. Training will be given to all M365 Copilot users to reinforce that they must review outputs before using/sharing them.

- The Panel queried whether it should be disclosed when content is created with assistance from CoPilot. For small tasks like drafting an email this may not be appropriate. As part of the ongoing business benefit discovery work ACC will seek feedback about the benefits/practicalities of disclosing when Microsoft 365 Copilot has been used.

- The Panel queried the data retention in place when using CoPilot, for example recording and transcriptions of meetings. These recordings are stored on the individual who recorded or hosted the session's OneDrive. All meeting members are automatically given access to the recording. However, the host or recorder of the session can both add and remove users, as well as delete the recording entirely.

- The Panel queried whether the tool would learn from requests made by staff. It was confirmed that it will not.

- The Panel advised consideration of whether there is any conflict in Microsoft providing this tool to a government/crown agency. Feedback was provided, there is no perceived conflict of interest regarding ACC taking part in the early access programme which was available prior to October 2023. ACC's involvement has been addressed with, and endorsed by, the Government Chief Digital Officer (GCDO). The Department of Internal Affairs CEO also contacted ACC's CEO and endorsement of ACC involvement was given.

- The Panel queried whether any other government agencies had trialled the tool, in particular agencies that carry less sensitive information than ACC, and whether any learnings from those agencies could be gained. No other government agencies have trialled this tool ahead of ACC. We are working closely with the GCDO, and they are wanting ACC to provide them with insights to help inform their guidance to other government agencies.

- The Panel queried the reported te reo Māori translations performed by the tool. It was noted that Microsoft have explicitly stated that te reo Māori is not a supported language for CoPilot and attempts at te reo by the tool should be thoroughly reviewed. It was also noted that the iwi dialect used when Copilot attempts a translation is unclear, and that transliteration is a closer description of what the tool attempts to do. The Panel clarified that computer generated translations are not encouraged, and that qualified and recognised translators should be used.

  Additionally, te reo translations should be peer reviewed by Māori partners or advisors for context. ACC's Māori Advisors and DCE Māori have agreed to the education and guidance we will provide users regarding Te Reo Māori and translation.

- The Panel queried whether CoPilot could generate images, and whether any images

would contain potentially identifiable and culturally sensitive information (for example, moko kauae or mataora). Copilot in PowerPoint can be asked to place images into PowerPoint – it sources these from Microsoft stock imagery. It cannot currently generate its own custom imagery and cannot alter existing images. It poses no additional risk as it operates exactly as searching and adding stock images manually.

- The Panel noted ACC's commitment to transparency in its use of AI; this should ideally include a page on the external website outlining what AI tools are used by ACC, how they are used, and what it will not be used for. They also suggested any resources to dispel myths about AI should be shared as widely as possible and the wider population (both ACC staff and the public, i.e. ACC's customers) are educated about the uses, risks, and benefits of generative AI tools in the workplace. See the 'Transparency, engagement, and communication' section below.

Transparency, engagement, and communication

Transparency is a key part of ACC's Generative AI Models and Services policy (see Appendix 1). ACC's External Engagement Team are working with the Generative AI Advisory Panel to place a relevant statement about ACC's use of Generative AI on ACC's public website.

ACC staff will be educated (via Intranet content and news posts) on the capabilities of Microsoft 365 Copilot and the scope of its use at ACC. Staff will be provided with a Copilot Terms of Use document and are made aware of the limited approved use cases that Copilot is to be utilised for. Staff will also be provided the opportunity to raise questions/concerns to the ACC Microsoft adoption team leading the use of Microsoft 365 Copilot, or to ACC's Generative AI advisory panel.

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. Stakeholders will include the Office of the Privacy Commissioner (OPC), GCPO, and other government agencies participants in the early access pilot.

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, particularly M365 Copilot. As such, ACC is consulting with relevant agencies such as Department of Internal Affairs to ensure that Microsoft365 Copilot is being operated by ACC in an open and transparent way.

The need for transparency also extends to ACC customers and clients, who would benefit from

the awareness of ACC using generative AI tools. Transparency provides clarity and reassurance, as to the extent and scope of M365 Copilot's integration, including the main mitigating control that Copilot does not integrate with ACC's client record systems.

Microsoft 365 Copilot will not be used at ACC for any activities tasks directly related to client care or resourcing provided to clients, customers, or providers. It will only be used to realise internal productivity benefits relating to supporting functions. If, in the future, it is decided to extend the use of Microsoft 365 Copilot to any activities related to client care or resourcing provided to clients, customers or providers, relevant community stakeholders will be consulted.

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 and the particular attention drawn to Māori protected materials.

Māori protected materials

ACC's internal Māori advisors have been consulted regarding risks associated with Māori protected materials being entered into Microsoft 365 Copilot. The primary risk of using Māori protected materials with Generative AI tools is the possible threat to the integrity of the materials, Māori control over the materials or the cultural, economic, or other potential benefits to Māori of the materials. It was agreed that this risk is mitigated by the fact that, unlike other generative AI tools, M365 Copilot cannot 'learn' from the prompts or information we use with it (or responses generated) or add that information to its corpus of knowledge.

ACC's internal Māori advisors have also agreed to the guidance provided to ACC users of Microsoft 365 Copilot regarding interpretation of te reo Māori and the need to consult with ACC's DCE Māori team for assistance when translating te reo Māori to ensure accuracy and cultural appropriateness. This ongoing commitment is evidence by the fact Māori protected materials are a primary consideration that has been implemented into ACC's Generative AI models and service policy statement,

Privacy Assessment

The Privacy Act 2020 provides a legal framework that ACC must adhere to. The below table summarises the key considerations of each privacy principle and assesses the compliance of Microsoft 365 Copilot against each principle.

#	Description of the privacy principle	Summary of personal information that is involved, its use, and the 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. Microsoft 365 Copilot does not collect any new personal information. It only collates and analyses information that has already been collected by ACC and that users have access to.	The use of M365 Copilot complies with principle one as it does not collect personal information.	
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. Copilot does not any new personal information from ACC's client systems. ACC staff are educated on what information is collected and from what systems in their M365 Copilot onboarding.	The use of M365 of Copilot at ACC is compliant with Principle Two. M365 Copilot does not collect information, nor does it access any of ACC's client management systems. Further to this, all client or staff personal information held by ACC has been collected for a lawful purpose and	
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 is 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.	ACC is not collecting new personal information by using M365 Copilot. However, ACC has social responsibility and transparency requirements as a government agency to ensure that both clients and staff understand the use and scope of generative artificial intelligence being used at ACC. ACC currently has a statement on its website outlining that Generative AI is undergoing testing at ACC. It has been noted that this will	R-001

			need to be updated when this undergoes full roll-out.	
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. There is no collection of any new personal information using M365 Copilot.	The use of M365 Copilot complies with Principle Four. No new information is being collected for the use of M365 Copilot, nor does it collect personal 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.	ACC has instigated a significant number of security and storage controls that vary from technical controls provided by Microsoft, ACC data governance controls, and staff member education. Multi-layered controls significantly reduce the risk of security concerns and ensures that ACC is compliant with Principle Five.	R-002
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.	The use of M365 Copilot complies with Principle Six. Individuals will be able to access their personal information in the same way as always. M365 Copilot does not change this process. M365 Copilot does not introduce any new storage methods, so all information produced by M365 Copilot will be accessible in the same was as other Microsoft documents.	
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.	The use of M365 Copilot complies with Principle Seven. There is nothing about the use of M365 that would change the way that ACC complies with Principle Seven. Individuals will be able to correct their personal information in the same way as always. M365 Copilot does not change this process. M365 Copilot does not introduce any new storage methods, so all information produced by M365 Copilot will be accessible in the same was as all other Microsoft	

			documents. Corrections can then be applied in the same way as they are for any other document.	
8	Principle Eight – Accuracy of personal information to be checked before use. Make sure that personal information is correct, relevant, and up to date before you use it.	Principle eight requires ACC to ensure that information is accurate and up to date before it is used.	There are a range of soft controls in place to ensure that outputs produced by M365 Copilot are accurate prior to being used. There remains risk that an output is not thoroughly reviewed, however this is not a risk inherent to the use of M365 Copilot and applies to all documents. There also remains risk of misuse where staff directly put personal information into M365 Copilot, causing misleading or inaccurate results.	R-003 R-004
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	The use of M365 Copilot complies with Principle Nine. There are existing retention guidelines in place and M365 Copilot has clear retention schedules and guidelines.	R-005
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. There are	The purposes for which information has been collected have not changed nor has the purpose for its use. It is the manner of processing that has changed. There are a range of soft controls in place to mitigate risks posed by using M365 Copilot at ACC. Currently ACC has a generative AI service policy and a M365 Copilot approach document that frame limited use cases for Copilot and restricts the use of personal information directly being put into prompts. Client information, personal data, or confidential content should not be directly put	R-006

			into M365 Copilot and is prohibited in the M365 Copilot terms of use. ACC staff are made aware of the limited use cases for using Copilot and that they are not permitted to input personal information directly into M365 Copilot prompts. ACC staff are to complete a review of the documents produced by M365 Copilot. There remains a risk that users do not comply with the policy and terms of use. However, this would be at odds with the ACC Code of Conduct and would be dealt with accordingly.	
11	Principle Eleven – Limits on disclosure of personal information. Only disclose it if you have got 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.	Some disclosures may occur from documents produced from M365 products, including SharePoint and Outlook. Documents are to go undergo human review prior to disclosure. Therefore, if M365 Copilot were to produce content that was incomplete, inaccurate, or that included personal information that should not be disclosed this should be detected.	R-007
12	Principle Twelve- Disclosing information outside New Zealand Only share information with an agency outside New Zealand if the information will be protected.	Principle twelve restricts the disclosure of personal information outside of New Zealand. Information may only be 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.	The use of M365 Copilot does not require disclosure outside of New Zealand. ACC has opted out ACC data being disclosed to, retained, or used by Microsoft and therefore is compliant with Principle 12.	R-008
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.	ACC is compliant with principle thirteen when using M365 Copilot. M365 Copilot does not assign unique identifiers. ACC has a policy that no personal information including unique identifiers should be inputted	R-009

			directly into the tool, nor does M365 Copilot store or use ACC data.	

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.

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	Residual risk remaining despite new safeguards.
R-001	ACC are not transparent about the use of generative artificial intelligences at ACC	ACC customers and clients lose trust in ACC	Moderate-Unlikely Medium	**Information Management** • Currently ACC has a statement on its external facing website that outlines the testing of generative AI as a tool at ACC.	Minor -rare Low	**Information Management** • For full roll-out of generative AI tools the ACC website should be updated with a general statement that generative AI tools are being used in certain areas of the organisation.	Minor-rare Low
R-002	ACC have not got appropriate storage and security practices in place that leads to	ACC client, staff, or customer information is lost, used, or disclosed.	Minor-possible Medium	**Data Governance** • M365 Copilot is unable to access ACC authoritative client systems.	Minor-rare Low		Minimal-rare Low

	loss of personal information.			• Access to personal information stored across Microsoft SharePoint will be subject to requisite user access permissions. • Incident register that records incidents to identify where data governance needs to be improved. **Information Management** • Prompt interactions are to be stored within ACC's tenancy. **People** • Managers asked to review their own access permissions when onboarded to a role. • Education campaigns in place that teach users best practice regarding file sharing and permissions. **Technology** • Prompt interactions from ACC staff are encrypted end-to-end as they are sent to and from the M365 large language model (LLM). • Microsoft/Azure Cloud is ISO 27001 certified, integrated with M365. • M365 Copilot has ACC internal Certification and Accreditation approval.			

				• Microsoft 365 uses service side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TSL) and Internet Protocol Security (IpSec).			
R-003	ACC uses information produced by Copilot that is inaccurate	Decisions made about clients or staff are informed by inaccurate information.	Minor-possible Medium	**Policy** • ACC's M365 Copilot Terms of use prohibits direct input of personal information into M365 Copilot. • ACC's M365 Copilot Terms of use prohibits use of Copilot to "determine care or resourcing provided to clients, customers, or providers. **Education** • Users complete training on how to accuracy check M365 Copilot outputs including source checking. **People** • Users are to complete an accuracy check for all work that is produced by M365 Copilot.	Minor-Unlikely Low		Minor-rare Low
R-004	ACC staff input personal information directly into Copilot and output is not	Inaccurate information produced by Copilot	Minor-possible Medium	**People** • Users are to review outputs of Copilot prior to their use.	Minor-unlikely Low	**Information Management** • If capability became available with ACC's	Minor-rare Low

	reviewed properly and could lead to inaccurate or misleading results.	pertaining to staff, client, or customer information.		**Education** • Users complete training on how to accuracy check M365 Copilot outputs including source checking. **Policy** • ACC's M365 Copilot Terms of use prohibits direct input of personal information into M365 Copilot.		current subscription, consider the addition of a spot check feature to ensure compliance.	
R-005	ACC retains information produced by M365 Copilot for longer than is necessary.	Clients or staff are unable to trust that their information will be retained in the required manner.	Minimal-Unlikely Low	**Policy** • ACC has retention guidelines for client record and staff personal information. **Technology** • M365 Copilot has clear retention schedules and guidelines that adhere to ACC's requirements. • ACC M365 Copilot Admins can request hard deletion for certain prompt interactions.	Minimal – rare Low		Minimal-rare Low
R-006	ACC uses information produced by M365 Copilot which was not to do with the purpose of the information's collection	Clients and staff are unable to trust that information collected about them is used for the purpose for which it was collected.	Moderate – Possible Medium	**Policy** • Currently ACC has a Generative AI Service Policy and a M365 Copilot approach document that frame limited use cases for Copilot and restricts the use of personal information	Minor-rare Low	**Education** • Maintain knowledge sessions with ACC about changes to M365 Copilot.	Minor-rare Low

				being put directly into prompts. **People** • ACC M365 Copilot Users are made aware of the limited use cases for using Copilot and that they are not permitted to input personal information directly into M365 Copilot prompts. • ACC M365 Copilot users are to complete a review of documents produced by M365 Copilot.			
R-007	ACC discloses inaccurate information produced by M365 Copilot		Minor – Unlikely Low	**People** • Users are to complete a human review prior to disclosure of ACC information. For AI produced content this review would be completed at the point of producing the document, and at the point of disclosing the document. **Policy** • ACC Generative AI Model and Services Policy requires users of generative AI products to complete a human review.	Minimal – Unlikely Low		Minimal – Rare Low
R-008	ACC discloses client or staff information to an agency outside of New Zealand		Minimal – Unlikely Low	**Technology** • M365 Copilot LLM does not learn from ACC data by default	Minimal- Rare Low		Minimal-Rare Low

				• M365 Copilot will not store any information outside of ACC's tenancy. • Web content interactions where M365 uses the input to query the web has been turned off. • Microsoft does not store or learn from prompt interactions from ACC users.			
R-009	Unique identifiers are assigned or used by M365 Copilot.		Minimal-Possible Low	**Policy** • ACC's M365 Copilot Terms of Use policy prohibit users from directly inputting personal information into prompts. **Technology** • M365 Copilot does not store or use ACC data. • M365 Copilot does not assign unique identifiers. • Copilot inputs encrypted in transit and at rest.	Minimal-Unlikely Low	**Information Management** • If it becomes possible to add a DLP to prohibit unique identifiers from being added this should be considered.	Minimal - rare Low

Action Plan

There are some ongoing actions to monitor using Microsoft 365 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
Education provided to users to ensure that M365 users are aware of terms of use and operating M365 responsibly.	Product Owner	Continuous
Advise Privacy if any changes to privacy risks or controls	Product Owner	Continuous
Monitoring of changes to M365 Copilot from Microsoft	Product Owner	Continuous
Update ACC website as uses of generative AI at ACC change	Generative AI Policy Owner	Continuous
Advise Privacy of any changes to PIA actions	Product Owner	Continuous

Ethics risk assessment

Number	Description of ethical risk	Control in place
1	Unethical outputs could be generated and used resulting in bias or discrimination.	M365 Copilot has been reviewed by the ACC Ethics Panel to identify any ethical issues with its use. ACC's staff will be made aware of the potential for bias or discrimination in Generative AI Model outputs and will be expected to mitigate these risks. Education is to be provided to all M365 Copilot users when they are onboarded to M365 Copilot about identifying and remove bias. All outgoing work should be peer reviewed; this includes documents produced by M365 Copilot. Development of a library of pre-prompts that allow users to outline the scope of the response expected from M365 Copilot to mitigate against biased responses e.g. "Please ensure the output covers a range of views and contexts".
2	Māori Protected Materials being entered into M365 Copilot threatening the integrity of the materials, Māori control over the materials, or the cultural, economic, or other potential benefits to Māori of the materials.	Unlike other generative AI tools, M365 Copilot cannot 'learn' from the prompts or information we use with it (or responses generated) or add that information to its corpus of knowledge. ACC Māori advisors have been consulted to ensure they are comfortable with Microsoft 365 Copilot's functionality and the controls we have in place for its use at ACC.

Risks Summary

The main privacy risks are privacy breaches of any personal information held by ACC. These breaches could include, storage and security of personal data (IPP5), accuracy (IPP8), and misuse (IPP10).

The risks of breaching client personal information are mostly alleviated because Microsoft 365 Copilot does not integrate with ACC's authoritative client record systems. Therefore, Copilot is unable to collect, use or disclose personal information from those systems.

There is a remaining privacy risk that Microsoft 365 Copilot may be able to recollect, summarise, and analyse any remaining personal information that is stored in Microsoft products such as SharePoint, Word, and Excel. However, there are several controls in place that largely mitigate privacy risk. These controls include access permissions, continual engagement and communications about SharePoint site access controls, and M365 Copilot terms of use that stipulates that personal information should not be directly input into M365 Copilot and that all outputs should undergo human review.

There is a remaining privacy concern regarding ensuring that users do not put personal information directly into M365 Copilot. In the future, if the feature becomes available in the current subscription version the Privacy team suggests considering implementing spot checking to ensure client personal information is not directly entered into the tool.

Human oversight will be a key element for ensuring that outputs of M365 are accurate and are used appropriately. Prior to use of M365 Copilot there should be an understanding of what humans will need to have oversight of, and how they ought to monitor the use of the tool. This has been implemented as an education session when users are onboarded.

Ethical concerns have been raised and addressed by ACC's internal ethics panel, and there is expectation that both ACC and Microsoft 365 will be adherent to the Responsible AI guidelines developed by Microsoft, and remain aware of developing AI regulations overseas, including the proposed EU AI Act 2025.

Benefits

The early phases of Microsoft 365 Copilot use at ACC will be used to identify actual business benefits that can be realised - however it is expected that the broad categories of benefits will include:

1. Reducing time and effort writing meeting notes
2. Lowering meeting costs by reducing who needs to be in meetings.
3. Reducing time and effort by using Copilot to summarise documents.
4. Reducing time by using Copilot to summarise email threads.
5. Speeding up content and email creation by asking Copilot to provide drafts.
6. Quickly generating ideas by asking Copilot to make recommendations.
7. Reducing time and improving reporting by using Copilot to visualise data, describe what information is telling us and form projections based on variables.

8. Reducing time and effort by getting Copilot to generate draft SharePoint pages.
9. Quickly discovering information by asking questions of Copilot chat

The ACC internal Ethics Panel also noted the accessibility benefits for people with difficulties around language and writing (e.g. dyslexia). Surveys done as part of the M365 Copilot pilot have indicated that it has been extremely beneficial. The benefits have included reducing stress about keeping up with meeting notes, being able to ask Copilot to repeat what was said in meetings, Copilot being able to improve written content, and alleviating anxiety and inertia of 'getting started'.

A Proof of Pilot phase survey has identified that 81% of users say Copilot helps improve the quality of their work, 80% say it allows them to complete tasks faster, and 77% said it makes them more productive. It has been identified as being particularly useful for finding content, summarizing meetings, refining content, and drafting content.

Conclusion and recommendations

The main privacy risks highlighted in this PIA surround access (IPP5), accuracy (IPP8) and misuse (IPP10). Overall, there are several 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 continually controlled with the use of Microsoft 365 Copilot.

- Staff Copilot users will need to be responsible for ensuring Copilot outputs produced are accurate before being used. Users complete training for accuracy when they are onboarded. This training includes how to prompt M365 Copilot well to ensure accurate answers, and how to then check the outputs for accuracy.
- If there are changes to the way that M365 Copilot in a way that impacts privacy, the ACC Microsoft Enablement team needs to liaise with ACC Privacy team to ensure that controls are in place to mitigate any risk that arises.
- In the case that use cases expand the ACC Microsoft Enablement team need to liaise with ACC Privacy team to ensure that no new privacy concerns arise because of a new use case.
- An assessment will be necessary from Information and Security and Privacy at ACC if it were proposed that web content is turned on.
- Ensure that ACC staff use M365 Copilot within the agreed use cases and that they not directly input personal information. If there is a change to the general terms of use this should be amended in the terms of use document and the Microsoft Enablement team needs to liaise with the ACC Privacy team to ensure that this change does not introduce new privacy concerns
- The Microsoft enablement team should audit SharePoint permissions, which is where M365 Copilot could be used to collate and summarise personal information.

References and resources

References:

Microsoft. “Encryption in the Microsoft Cloud”. Microsoft Learn. August 9, 2023. https://learn.microsoft.com/en-us/purview/office-365-encryption-in-the-microsoft-cloud-overview. Accessed January 26, 2023.

Accident Compensation Corporation. October 2023. ACC's pilot approach for Microsoft 365 Copilot.docx, October 2023. Accessed January 20, 2024.

Identify common concerns or commons areas of risk dent Compensation Corporation. Generative AI Models and Services Policy. Policy approved August 2023. Generative AI Models and Services Policy - Updated Review Date.pdf. Accessed 25 January 2024.

Microsoft. Responsible AI Standard, v2. June 2022. https://www.microsoft.com/en-us/ai/principles-and-approach?rtc=1 Accessed 27 January 2024.

Microsoft. Microsoft Privacy Statement. Privacy. Updated October 2023. https://privacy.microsoft.com/en-gb/privacystatement.Accessed January 24, 2024.

Microsoft. Data, Privacy, and Security for Microsoft 365 Copilot. https://learn.Microsoft.com/en-us/Microsoft-365-copilot/Microsoft-365-copilot-privacy. Accessed January 24, 2024.

Microsoft. Examine data security and compliance in Microsoft 365 Copilot. https://learn.Microsoft.com/en-us/training/modules/examine-data-security-Microsoft-365-copilot/.

ACC references/resources:

Generative AI Models and Services Policy.pdf

ACC's pilot approach for Microsoft 365 Copilot.docx

Stakeholder Report - Microsoft 365 Copilot Testing Results.docx

M365 copilot ethics panel feedback December 2023.docx

AI Controls Framework Comms.pptx

Copilot AI Controls.xlsx

Appendix 1 – ACC Generative AI Models and Services Policy Statements

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. **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 Models and Services 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.

Appendix 2 – Terms of Use

All users of M365 Copilot must agree to the following terms of use before being given access to it:

Terms of Use - M365 Copilot

Note: You can withdraw your consent at any time by emailing OfficeProductivity@acc.co.nz - we'll then remove you from the pilot group and reallocate your M365 Copilot licence to someone else.

Hi, Shelly. When you submit this form, the owner will see your name and email address.

1. I agree to the following:

   I will not use M365 Copilot for purposes which are related to client care or involve the entry of personal or health information.

   I will not use M365 Copilot for activities which determine care or resourcing provided to clients, customers or providers.

   I will not include client information, personal data or confidential information in the prompts I enter into M365 Copilot.

   I will review and approve all outputs created by M365 Copilot before sharing or acting upon them.

   I will test proposed evidence-based results by independently checking references and evidence for validity.

   I will take ethical considerations into account when using M365 Copilot.

   If you use M365 Copilot to assist you to formally translate, analyse or produce Te Reo Māori content please consult with the DCE Māori team to ensure your resulting work is accurate and culturally appropriate.

   If I am in doubt over the use of M365 Copilot for a particular purpose I will check with the Ethics/Privacy Team.

   If I have questions or concerns relating to intellectual property use I will direct these to the ACC Legal Team.

   If I have any questions or concerns regarding the use of M365 Copilot with Mātauranga Māori, tikanga, or taonga (Māori Protected Materials) I will direct these to the DCE Māori team.

   I will report any misuse or potential security or privacy incidents involving M365 Copilot to my manager.

Appendix 3 – ACC's Generative AI Controls that relate to M365 Copilot

Control title	Control description	Control Operator	How this will be addressed for M365 Copilot
Awareness of legal and regulatory requirements	On a quarterly basis the Control Operator will monitor and document any changes in ACC's strategic direction with regards to AI legislative and/or regulatory requirements and the potential impact on ACC and its AI Systems and Services. The documented changes and impact will be shared with the AI Governance Group for further consideration and potential action	ACC Legal Team	If Governance group makes changes based on regulatory changes, we will reassess M365 Copilot in light of these changes.
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 AI Governance Group for consideration.	Product Owner	As part of our standard evergreen monitoring process, we will review and update our user resources and training to ensure they meet current guidelines and best practices for trustworthy AI. Feedback will be provided to the AI Governance Group for consideration.
AI Risk Management Process Review	On a 6-monthly basis, the Control Operator will conduct a comprehensive review of the AI risk management process. This will include: - An evaluation of the effectiveness of existing controls - Alignment with organisational objectives and regulations, - Identification of potential improvements - A detailed report outlining findings and recommendations to the Enterprise Risk team and the AI Governance Group	Enterprise Risk	The M365 Copilot Product Owner will provide input as required into reviews.

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.	Architecture team; Information Security team	As part of any solution selection and approval process, the Architecture team should flag new systems on our system register as approved applications/ AI platforms. This is not related specifically to M365 Copilot.
Certification and Accreditation	Review the required sample and confirm that: Solution C&A's were certified by the CISO Solution C&A's were accredited to operate by the CTIO C&A packs and approvals were stored on a secure Security shared drive Meetings are being held	Information Security Team	We will follow the documented C&A process.
AI Risk Management Roles and Responsibilities	On an annual basis the Control Operator will review: - 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.	Enterprise Risk Team	Our terms of use for M365 Copilot will reference roles and responsibilities.
Staff AI Risk 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.	Privacy Team	ACC learning modules will be developed to address AI training and to monitor who has completed the modules. M365 Copilot-specific onboarding will be taking place.

AI System testing	On a quarterly basis, the Control Operator will verify the appropriateness and effectiveness of the testing process of AI Systems by reviewing the outcomes of testing that has taken place over the past 3-months. Where identified, the testing process will be realigned and/or guidelines for testing will be further reviewed.	Product Owner	Initial testing takes place when we release a new system, when there are significant changes, or there is a release of new features that require retesting. Regular retesting of an existing solution is not generally performed. The outcomes of any M365 Copilot testing that has been performed can be provided as input into the broader testing process/guidelines, if required.
Stakeholder & User feedback	On a quarterly basis the Control Operator will review and verify that stakeholder feedback is considered and appropriately addressed as outlined in ACC's AI Policies	AI Governance Group	Product Owner requires a mechanism to be put in place to collect user feedback. Feedback reports can be provided to the AI Governance Group, if relevant.
AI 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	AI Governance Group with support of Audit team	The M365 Copilot Product Owner will provide input as required into reviews.

Appendix Four: Map of Microsoft Copilot Products