M365 Copilot Privacy Impact Assessment

Te Kawa Mataaho
Public Service Commission

Contents

1. Document Control: 1
2. Executive Summary 1
3. Overview and Purpose 2
4. Background and approach 2
5. Policies and guidance relevant to this PIA 6
6. Scope of this PIA 7
7. Approach for this PIA 8
8. Privacy-Relevant Characteristics of Microsoft 365 Copilot 8
9. Personal Information in Scope 8
10. Assessment of privacy risks and mitigations in place 10
11. Privacy Principles Assessment 13
12. Conclusion 15
13. Supplementary resources 15
14. Appendices 16

1. Document Control:

Version	Document Status	Responsible	Comments
0.1	Draft	Hayley Kinsey	Initial draft
0.2	Draft	Hayley Kinsey	Amendment to address comments from Legal/DCE review
0.3	Draft	Hayley Kinsey	Further amendment to address comments from Privacy Officer review
0.4	Draft	Hayley Kinsey	Risk workshop with SRO/CIO to establish ratings
1.0	Approved	Thor Gudjonsson	Approved, 9 April 2026

2. Executive Summary

This Privacy Impact Assessment assesses the privacy implications of the Public Service Commission's proposed use of Microsoft 365 Copilot. This assessment is intended to be read as a stand-alone document while explicitly relying on, and not duplicating, the findings of the existing Privacy Impact Assessment for Microsoft 365.

The Microsoft 365 PIA establishes the baseline privacy position for the Commission's Microsoft 365 tenant, including platform-level risks, governance arrangements, and compliance with the Privacy Act 2020. This PIA focuses solely on whether the introduction of Copilot materially alters those risks or introduces new privacy considerations.

Copilot generates responses based on user prompts and content that the user is already authorised to access within Microsoft 365. The principal privacy impact of Copilot arises from its ability to surface, summarise, and synthesise existing information more efficiently, which may amplify existing risks associated with information access, over-sharing, use for an unauthorised purpose, misclassification, over-retention, and human error.

The deployment of Microsoft 365 Copilot within the Public Service Commission introduces several privacy risks that require careful management. Copilot amplifies existing privacy risks by surfacing and synthesising data already held within the Commission's Microsoft 365 environment.

Key risks include unauthorised access to sensitive information, inadvertent disclosure through AI-generated outputs, over-sharing or use for unintended purposes, misclassification and over-retention of data, and human error in prompt creation or response handling. Additionally, prompts and responses generated by Copilot are stored within users' Outlook profiles, which may retain personal or organisational information and thus require robust governance, user guidance, and controls.

Provided that these safeguards are effectively implemented, the use of Copilot remains consistent with the Privacy Act 2020 and aligns with the expectations of the Office of the Privacy Commissioner for responsible AI use.

3. Overview and Purpose

Microsoft 365 Copilot is an AI-assisted capability embedded within Microsoft 365 applications such as Word, Outlook, Teams, and SharePoint. It is a productivity tool that utilises large language models to generate content across Microsoft365 apps such as Word, Excel, Teams, and PowerPoint. It assists users by drafting content, summarising information, answering questions, and generating insights using organisational data to which the user already has authorised access. The information sources and integrated applications are listed in Appendix A.

The purpose of this Privacy Impact Assessment is to:

- assess whether the use of Microsoft 365 Copilot materially changes how personal information is accessed, used, or disclosed within the Commission's Microsoft 365 environment
- identify privacy risks specific to AI-assisted search, aggregation, and content generation
- confirm how existing privacy management practices apply to Copilot
- identify any additional safeguards required to ensure continued compliance with the Privacy Act 2020

This assessment has been undertaken in accordance with guidance issued by the Office of the Privacy Commissioner, which emphasises the importance of completing a Privacy Impact Assessment before deploying AI tools that interact with personal information.

4. Background and approach

Generative AI tools and their use across the Commission

Generative AI tools such as Microsoft 365 Copilot provide efficiency enhancements that allow Public Service Commission staff to focus on the things that matter. Generative AI tools accelerate

content creation, help staff with repetitive tasks and quickly surface relevant organisational insights.

It is important to emphasise that GenAI does not replace the need for human review, input, or decision-making—rather, it enhances our capacity, allowing people to focus on higher-value activities while maintaining oversight and judgement.

Responsible AI usage

The PSC AI Policy specifies that staff must:

- Use only approved AI solutions for Commission work
- Handle information appropriately when using AI, protecting security and privacy
- Apply critical thinking and human oversight, treating AI as a support tool, not a decision-maker
- Use AI ethically, lawfully and fairly
- Report issues immediately

Staff remain fully accountable for their mahi and any decisions made, even when AI is used. Formal acceptance of this policy is required to use Generative AI. Non-compliance with policy may result in disciplinary action.

M365 Copilot

Copilot is Microsoft's Generative AI solution. M365 Copilot is able to integrate with existing Microsoft products such as SharePoint, Outlook and the Office suite. A full list of applications currently integrated with Copilot can be found at **Appendix A**.

Microsoft 365 Copilot acts as an intelligent assistant by leveraging advanced AI models to process and interpret data available within the organisation's Microsoft 365 environment. It uses information that users are already authorised to access, including emails, documents, meetings, and chats, to generate tailored content, provide contextual summaries, and surface relevant insights.

Copilot adheres to Microsoft's Responsible AI principles, ensuring the product developed takes into account fairness, reliability and safety, privacy and security, transparency, accountability and inclusiveness.

How Copilot works

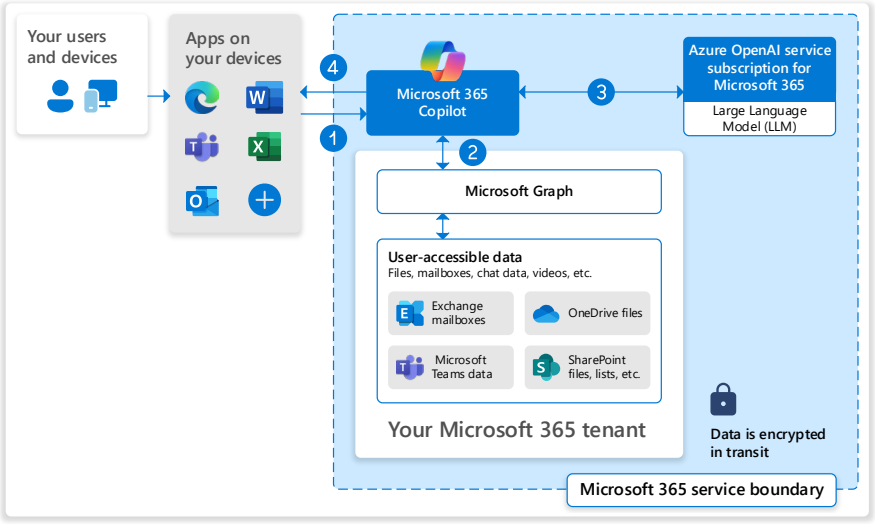


Diagram 1 shows how a prompt is processed through Copilot

1. In a Microsoft 365 app, a user enters a prompt in Copilot.
2. Copilot preprocesses the input prompt using grounding and accesses Microsoft Graph within the Public Service Commission's Microsoft tenant.
    - Grounding improves the specificity of prompts and helps users get answers that are relevant and actionable to their specific task. The prompt can include text from input files or other content Copilot discovers.
    - The data Copilot uses to generate responses is encrypted in transit between the PSC data source and the Copilot LLM, this uses Tl1 encryption.
    - Copilot data is processed in the M365 data centres within our specified geographical region (Australia).
3. Copilot sends the grounded prompt to the large language model (LLM). The LLM uses the prompt to generate a response that is contextually relevant to the user's task.
4. Copilot returns the response to the app and the user.

Copilot access to Public Service Commission data

Microsoft 365 Copilot has access to a broad range of data across the Commission's Microsoft 365 environment, specifically leveraging information stored within applications such as Word, Outlook, Teams, and SharePoint.

This includes emails, calendar events, documents, spreadsheets, presentations, chat messages, meeting notes, and files stored in OneDrive and SharePoint sites. Copilot interacts only with data that individual users are already authorised to view, ensuring that existing access permissions and security controls are respected throughout all its operations. By drawing from these integrated data sources and storage locations, Copilot enables tailored content generation based on access permissions.

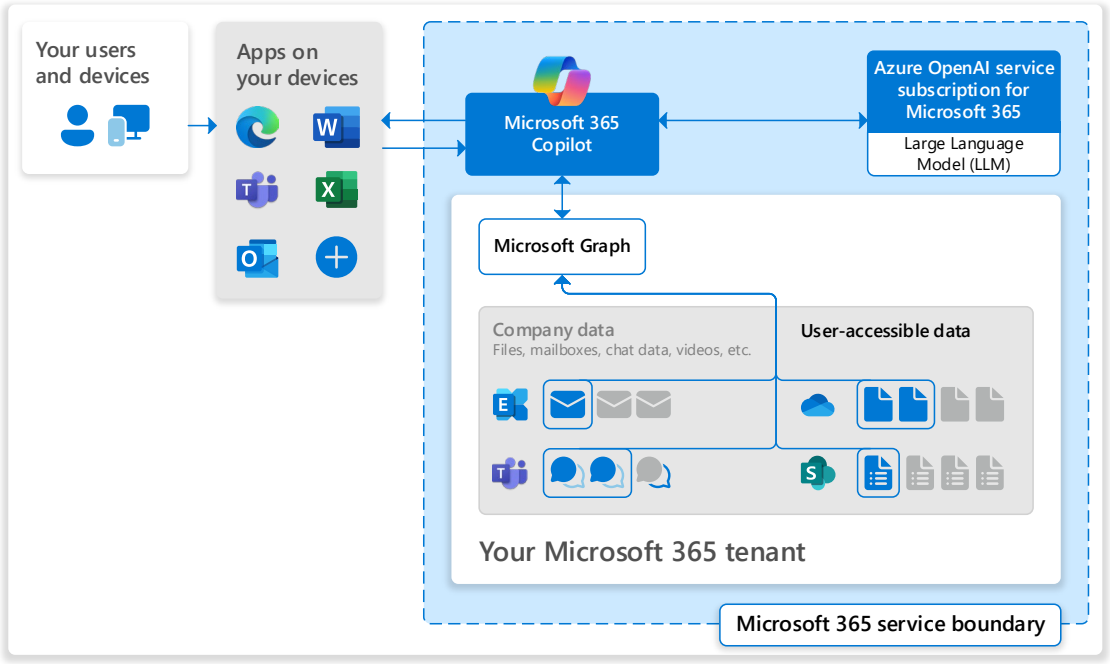


Diagram 2 demonstrates how Copilot respects user permissions to data

How we ensure our data is secure and protected

Data held on the Public Service Commission M365 environment is tightly controlled by preventative security policies and controlled access permissions. Both the M365 environment and Copilot functionality have been through Certification and Accreditation to ensure they are compliant with Protective Security Requirements.

M365 Copilot has enterprise data protection and adheres to the service boundary, ensuring data used in prompts is end-to-end encrypted and no Commission data is used for the training of the large language model (LLM).

Copilot data artefacts and retention

Current retention period for prompts is indefinite, unless manually deleted. Teams recordings expire from view after 90 days but are currently retained indefinitely. Both of these can be manually deleted by the user. Further analysis is being undertaken to consider the retention policies and auto-deletion policies of these holdings, and may be changed in the future.

Understanding the M365 Service Boundary vs the Tenancy Boundary

The **M365 service boundary** defines the overarching security and operational perimeter managed by Microsoft for all customers utilising Microsoft 365 services. This boundary encompasses the infrastructure, data centres, and systems that Microsoft operates to deliver services such as Outlook, Teams, SharePoint, and OneDrive, thereby ensuring that data remains within Microsoft's secure environment.

The **tenancy boundary** refers to the distinct partition allocated to each organisation within the Microsoft 365 environment. All data, files, and configurations associated with an organisation are segregated from those of other tenants, ensuring that access is restricted to users who are part of that specific tenancy and authorised accordingly.

The service boundary can be likened to the structural walls of a secure building, representing Microsoft's responsibility for the protection of the overall environment. The tenancy boundary, meanwhile, acts as a private office within that building, reserved for a particular organisation, where access and data management are governed internally. This distinction supports both privacy and control of organisational data within the broader Microsoft cloud infrastructure.

High risk Commission data

Copilot is blocked from accessing our most sensitive data, including anything marked as [RESTRICTED] and a small number of sites that have been determined to be of high risk (see **Appendices C, D** and section 10 of this PIA for more information).

Restricted documents are the highest classification we are certified to hold at the Commission. The number of these documents currently stored on SharePoint is very low (under 30 documents formally classified as Restricted, but likely more that have been uploaded and not formally labelled in Sharepoint). Restricted documents generally reside in small numbers of users' outlook accounts.

For any other classified document, Copilot alerts the user that the information has come from a classified document.

Where is Copilot data stored?

Copilot data (prompts and outputs) is stored in user's mailbox. If needed for an investigation or disciplinary issue, information management staff can access prompts and responses using administrator tools, but only until they have been deleted in accordance with the retention rules.

Geographically, our Microsoft tenancy data is stored in near-shore facilities on the Microsoft servers (PSCs Microsoft geographic region is Australia). This is where data from users Copilot conversation histories will be held while retained and is aligned with GCDO's Cloud First policy.

Copilot by default provides some protection against

- Attempts to bypass safeguards
- Inappropriate or unsafe requests
- Requests involving protected, personal or restricted material
- Prompt injection and jailbreak behaviour

5. Policies and guidance relevant to this PIA

The Commission has an established privacy management framework that applies consistently across its information systems and business processes. These practices are documented in the Microsoft 365 PIA and include:

- an organisation-wide Privacy Policy
- defined processes for access and correction requests
- established privacy breach management and notification procedures
- use of Privacy Impact Assessments for new or materially changed uses of personal information

- staff training and guidance on privacy obligations and information management

These practices apply equally to the use of Microsoft 365 Copilot. Copilot does not displace existing accountability arrangements or decision-making responsibilities. Human judgement, professional responsibility, and compliance with Commission policies remain central to the handling of personal information.

Process for correcting issues and accessing Restricted data

- Staff will be advised in training of the process for raising issues such as incorrect permissions, inappropriate or concerning Copilot behaviour or misuse, or security issues should be reported to the CIO to deal with
- Privacy breaches should be reported to the Privacy Officer
- Assessment of serious-harm thresholds: The Privacy Officer will be responsible for determining when the threshold for serious harm is met.
- If people want to use Copilot to reason over Restricted information, they can seek permission to do this from the CSO via there manager.
- These procedures are also included in the Terms of use that staff have to accept before their licence will be issued.
- Log review procedures: Currently, log reviews are conducted on an ad hoc basis, with ongoing development under C&A initiatives.

6. Scope of this PIA

5.1 In scope

This PIA considers:

- the use of Microsoft 365 Copilot by Commission staff within Microsoft 365 applications
- user prompts and Copilot-generated outputs that reference or summarise organisational content
- privacy risks arising from AI-assisted discovery and aggregation of existing information
- governance, policy, and guidance relating to Copilot use

5.2 Out of scope

This PIA does not assess:

- Microsoft 365 or Azure at a platform or infrastructure level
- Microsoft’s training of foundation models
- Copilot use outside the Commission’s Microsoft 365 tenant
- individual business processes that are subject to separate PIAs

5.3 Reliance on existing platform-level assessments

This assessment relies on the findings of the Microsoft 365 PIA for matters relating to cloud service provider obligations, contractual safeguards, data residency, and tenant-level configuration. Those matters are not re-assessed here.

7. Approach for this PIA

This assessment builds on the evidence base established for the Microsoft 365 PIA and focuses specifically on Copilot-related changes. The approach included:

- review of Microsoft documentation describing how Copilot interacts with Microsoft 365 data
- consideration of Office of the Privacy Commissioner guidance on artificial intelligence and the Information Privacy Principles
- analysis of whether Copilot alters previously identified privacy risks or introduces new failure modes
- consideration of the guidance issued by GCDO on using AI responsibly in the Public Service

8. Privacy-Relevant Characteristics of Microsoft 365 Copilot

From a privacy perspective, Microsoft 365 Copilot:

- operates only over content the user is authorised to access
- does not bypass permissions or access controls
- does not create a new centralised repository of organisational data
- generates outputs accessible only by the user that may constitute personal information where individuals are identifiable

Copilot functions as an additional interface over existing information rather than as a new collection or storage mechanism.

9. Personal Information in Scope

The categories of personal information accessible through Copilot are the same as those identified in the Microsoft 365 PIA, including:

- **PSC Employees** - Identity and contact details; employment, payroll, performance, health and safety, and IT access information.
- **Workforce Data (System-wide) -**Aggregated and individual-level workforce information received from public service agencies, including demographics, employment characteristics, remuneration, and seniority. (The majority of this data is collected and stored via another platform, Snowflake which will not accessible through Copilot. However, some unit level data is stored in Sharepoint and this will be accessible through Copilot.)
- **Chief Executives and Senior Leaders -** Appointment, performance, remuneration, conflict of interest, and employment information for Public Service chief executives and senior leaders.
- **Inquiries and Reviews -** Identity and role information, allegations, evidence, findings, and recommendations collected in the course of statutory inquiries, reviews, and integrity functions.
- **Public Engagement and Research -** Contact details, survey responses, feedback, and submissions provided by members of the public and stakeholders.

- **Sensitive information held by the Crown Response Office -** Abuse in care survivor information, redress information.

Copilot-generated outputs may constitute personal information where they identify, describe, or are reasonably capable of being associated with an individual. This includes generated or summarised information, consistent with guidance from the Office of the Privacy Commissioner.

10. Assessment of privacy risks and mitigations in place

The following Copilot-specific risks have been identified. These risks amplify, existing risks documented in the Microsoft 365 PIA. Risks have been assessed against the PSC risk matrix. A summary of controls can be found at **Appendix E.**

	Risk	Risk level if no controls in place	Existing controls in place to mitigate risk	Assessment of residual current risk	Recommended additional actions to reduce or mitigate privacy risk	Residual risk level
R-001	Insufficient transparency of AI use in Commission, which may undermine public trust or confidence if not addressed proactively.	**17 High** (Moderate, Likely)	• PSC AI policy and guidance clear on what staff can and cannot use Copilot for. • Privacy impact assessments completed for both M365 and Copilot.	**13 Moderate** (Moderate, Possible)	• Publish a statement as part of or alongside the current privacy statement on the website to let the public know how AI is used in the Commission, including that Commission information, including any personal information we hold, is not used to train any LLM models. • Additional clauses in privacy statements when collecting new data explicitly stating that AI may be used in interpreting data. • Establish periodic review of Copilot use cases and privacy impacts as part of business-as-usual governance.	**5 Low** (Minor, Unlikely)
R-002	Over reliance on AI-generated outputs without sufficient human review, potentially affecting accuracy, context, or introducing bias particularly in sensitive matters.	**17 High** (Moderate, likely)	• All staff must accept PSC AI Policy and terms of use **(Appendix F)** prior to being granted a Copilot license. The policy specifies all AI-generated content must be reviewed by staff before use. Failure to comply with policy may result in disciplinary action. • Staff must check AI outputs for accuracy, bias, appropriateness, relevance, and context, verify any personal or sensitive information against the original source, and remain accountable for all final decisions and use of the content. • Staff additionally complete mandatory Copilot training before receiving a license, which includes checking outputs and sources.	**9 Moderate** (Moderate, Unlikely)	• Establish periodic reviews of our AI policy and acceptable-use guidance for Microsoft 365 Copilot, including expectations for prompt hygiene and mandatory human review of outputs. • Ongoing educations/comms to remind staff	**9 Moderate** (Moderate, Unlikely)
R-003	Unauthorised disclosure of personal information as a result of errors in the permission settings (i.e. users have access to documents containing personal information that shouldn't be disclosed to them)	**High 18** (Major, Possible)	• SharePoint access permissions are restricted to specific teams/roles in sites with sensitive information (e.g. human resources). • A review was undertaken of all sites by the Information Management Advisor. The sites containing the most sensitive data identified during this review, were reviewed by site owners prior to implementation to confirm correct staff members have access to these sites, reducing the risk of incorrect permissions. (see **Appendix B** for a list). However, the review only applied to those sites identified as the most sensitive – this means there are sites within SharePoint that have not been the subject of any review (see bullet point 2 of further remediation) • Highest risk data sites as identified by site owners blocked from Copilot. See **Appendix C** for a list of these sites. • Additional sharing of documents in sensitive sites now locked to named individuals only. This reduces the risk of unintentional oversharing of potentially sensitive information. However, a risk remains that the review may have missed errors in permission settings. • Te Mana Arataki, Managers and Digital Services given Copilot license prior to Commission wide rollout to test for anomalies and ensure Copilot behaviour with SharePoint integration meets expectations. We have had ongoing feedback over the course of manager testing and rectified any perceived errors (the majority of these related to misunderstanding the tool, permissions that were given that the user had forgotten they had access to and user error). We have also received	**13 Moderate** (Moderate, Possible)	• Establish periodic review of Copilot use cases and privacy impacts as part of business-as-usual governance. • Expand the review of sites to remainder of SharePoint to ensure all sites have correct permissions. • Establish a process to review permissions as part of BAU process. (e.g. when staff move roles). • Periodic spot check of permissions. • When new SharePoint sites are set up, Information Management team will require confirmation about whether Copilot should have access to this information. • Implement new sensitivity labels for teams who need Copilot for their day-to-day roles but share information wider across the Commission. This will allow team members to use the information with Copilot, but block staff members from outside these teams from using Copilot with the information to reduce likelihood of this accidentally being included in a response. See **Appendix D** for the details of teams requesting this functionality. • New sensitivity label tags available to staff that will enable targeted blocking of Copilot on specific documents, e.g. [IN-CONFIDENCE, NO COPILOT] tag.	**5 Low** (Minor, Unlikely)

			written acceptance of the tool (validation of the questions asked in testing script) from 8 managers (as at 9 April 2026), including from CRO. • Staff required to do annual Protective Security Requirements training including classifications refresher, as per current practice. • Staff required to report instances of Copilot providing responses that include information they should not have access to. • Mandatory training includes guidance of what to do if information is surfaced that the user shouldn't have access too.			
R-004	Copilot retrieves classified information as part of a response, which is then unintentionally included in an unclassified output.	**18 High** (Major, Possible)	• Highest sensitivity label – [R*STRICTED] blocked from being reasoned over by Copilot. In addition, another control has been introduced, whereby any email or document that hasn't been classified via sensitivity label, but contains the text string [R*ESTRICTED] in it, is also blocked. This will mitigate the highest risk documents. • Copilot signals the document classification of sources by displaying the shield icon in the colour relating to the label and in the response. • Staff are trained to look for sensitivity labels in mandatory Copilot training before license is applied. • PSC AI Policy and AI terms and conditions require staff to review outputs and ensure that sensitivity labelling is applied appropriately in any content created from the Copilot output.	**9 Moderate** (Moderate, Unlikely)	• Ensure annual classification training by security team mentions Copilot outputs as part of training collateral. • Consider mandated classification of all new records to increase awareness of classification labels.	**9 Moderate** (Moderate, Unlikely)

R-005	Prompt-based aggregation of personal information, where multiple data sources are unintentionally combined into a single output.	**9 Moderate**
		
		(Moderate, Unlikely)
			• PSC AI policy and terms of use **(Appendix F)** specify:
			  ○ Staff members must verify any personal or sensitive information against the original source, both in terms of accuracy and lawful purpose.
			  ○ Staff remain accountable for all final decisions and use of the content.
			• Microsoft has core privacy principles built into Copilot which provide some protections.
			• Checking outputs for appropriate use of personal data is included in the mandatory Copilot training. Training reinforces expectations under AI Policy and terms and conditions.
				6 Low
				
				(Moderate, Rare)
					• No further action required.	**6 Low**
						
						(Moderate, Rare)

R-006	Personal data is used for a purpose other than what it was collected for.	**High 18** (Major, Possible	• PSC terms of use and the mandatory training specify staff members must verify any personal or sensitive information against the source and only use the information in line with the purpose for which it was collected. • Sensitive folders for CRO and investigations have been scoped out of Copilot use. Other sites have had their sites reviewed and limited, reducing the likelihood of sensitive data being used for purposes it wasn't collected for. • PSC internal privacy policy specifies data may only be used for its intended collected purpose in line with the Privacy Act.	**13 Moderate** (Moderate, Possible)	• HR and Legal folders to have further restrictions added soon after launch, to protect these files further, limiting copilot use to only team members from relevant teams. • Ongoing training for staff around good information management controls, such as labelling etc, as well privacy training to ensure staff have clarity on their obligations with regards to Privacy Act	**6 Low** (Moderate, Rare)
R-007	Outdated data stored in SharePoint is surfaced in a response.	**8 Low** (Minor, Possible)	• Staff must verify sources and outputs from Copilot to ensure they are up to date and correct. • Mandatory Copilot training includes information management section, which reiterates importance of good information management hygiene. • Terms and conditions of use will reinforce requirements. • Copilot by default surfaces most relevant data (taking into consideration date created).	**4 Low** (Routine, Possible)	• Mandatory Copilot training to be added to onboarding process to ensure staff understand how outdated information will affect Copilot responses, e.g. utilising version history as opposed to making multiple versions of a document with different names. This is a prerequisite for allocation of the full license. • Disposal of documents should be automated in future to ensure documents are automatically deleted after retention period has passed. This will reduce reliance on manual deletion across SharePoint.	**2 Very Low** (Routine, Unlikely)

					• Good information management practices refresher training offered annually to all staff.	
R-008	Copilot creates a new record (chat/document) containing private or sensitive information when responding to prompts, which is then stored or handled incorrectly.	**1 Very Low** (Routine, Rare)	• Copilot chats and records are locked to the user interacting with Copilot. • Copilot is a tool designed to generate outputs for further use in a subsequent product/artefact (such as email, document etc). • Conversations within the retention period will be subject to the Official Information Act and Privacy Act while they exist. • The user can decide to retain or delete conversations after consideration of disposal authorities.	**1 Very Low** (Routine, Rare)	• No further action required. • Explore whether Copilot produced records may be automatically deleted or retained at the conclusion of the default retention period, if in line with either the general or specific disposal authorities.	**1 Very Low** (Routine, Rare)
R-009	Intentional misuse by a trusted insider	**15 Moderate** (Severe, rare)	• All staff with access to Copilot have signed the terms and conditions and agreed to the AI policy and Terms of Use of IT systems in the Commission. Any deliberate misuse of Copilot is classed as a breach of policy and may result in disciplinary action. • Most sensitive data locked to small number of individuals, reducing threat footprint. • If suspected misuse has occurred, and an investigation ensues prompts may be audited using information management tools. • Staff are informed during mandatory training that information contained in Copilot is logged and monitored, this should act as a deterrent to staff thinking they can get away with stealing data. • Built in prevention against malicious prompt injection and jailbreaking attempts standard with Copilot. • Existing PSR screening processes on hiring.	**6 Low** (Moderate, Rare)	• Assess data loss prevention policies in M365 (existing action in M365 PIA). • Explore further opportunities to report/alert of Copilot usage within Purview.	**6 Low** (Moderate, Rare)
R-010	Copilot is exploited in a cybersecurity incident by an external bad actor	**15 Moderate** (Severe, rare)	• In addition to the existing M365 certification and accreditation, a separate Copilot Certification and Accreditation has been done, with any critical remediations to be completed before sign-off.	**15 Moderate** (Severe, rare)	• Copilot Certification and Accreditation non-critical remediation activities to be completed in stated timeframes. • Ongoing security initiatives, as part of BAU, continue to strengthen security posture over time to respond to threat landscape.	**10 Moderate** (Major, rare)
R-011	Unethical outputs could be generated and used resulting in bias or discrimination	**13 Moderate** (Moderate, Possible)	• Human review is required by staff and users are accountable for final outputs. • Training material and policies explicitly detail that AI is not a decision maker. • Unconscious bias training modules are completed by staff. • Commission guidance and quality assurance templates for Ministerial advice expect peer review and management sign-off prior to finalisation.	**6 Low** (Moderate, Rare)	• Further training developed for writing effective prompts, ensuring AI considers other views and checks for bias. To be developed with partner vendor as part of programme of work and included in advanced prompting sessions.	**3 Very Low** (Minor, Rare)
R-012	Copilot is used for cultural advice or translation, resulting in misunderstanding or offense	**13 Moderate** (Moderate, Possible)	• This use of AI is not allowed under PSC AI policy, and a reminder of this is included as part of the mandatory training session to gain a Copilot license. • Staff to consult with cultural advisors or official translation services instead.	**9 Moderate** (Moderate, Unlikely)	• No further action required.	**9 Moderate** (Moderate, Unlikely)

11. Privacy Principles Assessment

This assessment adopts the same Information Privacy Principle-by-Principle structure as the Microsoft 365 PIA. This table on the following page describes any additional considerations above and beyond what the M365 environment introduces.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1, 2, 3, 4	• **Principle 1 - Purpose of the collection of personal information** Only collect personal information if you really need it • **Principle 2 – Source of personal information** Get it directly from the people concerned wherever possible • **Principle 3 – Collection of information from subject** Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it. • **Principle 4 – Manner of collection of personal information** Be fair and not overly intrusive in how you collect the information Take particular care if collecting information from children or young people	Microsoft 365 Copilot does not collect any new personal information. It only collates and analyses information that has already been collected by PSC and that users have access to.	**Compliant**. The use of Microsoft Copilot complies with principles 1, 2, 3 and 4 as it does not collect personal information.	**R-001** **R-006**
5	• **Principle 5 – Storage and security of personal information** Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	Copilot itself does not store within the tool, however, a record of prompts and responses is stored in the users Outlook mailbox in a hidden folder. See M365 PIA for controls around storage and back-ups of data held. In relation to access by Copilot to ensure compliance: • Sites containing sensitive data are locked to only staff requiring access by permission control. Copilot adheres to user's permissions when accessing files and generating responses. • The AI policy mandates staff review of outputs to ensure information sources are checked to ensure information is used for its intended purpose and not unduly disclosed. • Staff must report any permission anomalies that are uncovered by Copilot. • Misuse of information will be considered a policy breach and may result in disciplinary action.	**Compliant**. Principle 5 is largely managed by controlled access, with appropriate additional back-up controls in case of incorrect permissions applied to a document. Misuse or unintended disclosure of information may be managed through HR processes.	**R-003** **R-004** **R-005** **R-006** **R-009** **R-010**
6	• **Principle 6 – Access to personal information** People can see their personal information if they want to	• No new information being collected in Copilot implementation. • Personal information about an individual may be held temporarily in prompt/conversation history log in the user's Outlook. This is currently retained indefinitely. This data will be available to information management administrators to consider in responses to requests for individual data or OIA as appropriate.	**Compliant.** Data is not collected. Prompts can be surfaced when requested.	**R-008**
7	• **Principle 7 – Correction of personal information** They can correct it if it's wrong, or have a statement of correction attached	• Corrections will be addressed in source documents and eventual outputs where necessary. Copilot prompts and conversations are working documents which are only retained for 30 days, not official records that would require correction.	**Compliant.**	**R-007**
8	• **Principle 8 – Accuracy etc. of personal information to be checked before use.** Make sure personal information is correct, relevant and up to date before you use it	• Staff must check AI outputs for accuracy, appropriateness, relevance, and context, verify any personal or sensitive information against the original source, and remain accountable for all final decisions and use of the content.	**Compliant.** Ensuring accuracy remains a procedural responsibility supported by staff training and mandated by PSC AI policy.	**R-002** **R-007** **R-011** **R-012**

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
9	• **Principle 9 – Not to keep personal information for longer than necessary.** Get rid of it once you're done with it	• Retention periods for source documents and outputs sit within M365 tenancy settings, which have been addressed in the M365 PIA. • Copilot prompts and conversations are retained for 30 days, at which point they will be disposed of.	**Compliant.** Information disposal of prompts set to be automatically deleted.	**R-007** **R-008**
10, 11	• **Principle 10 – Limits on use of personal information.** Use it for the purpose you collected it for, unless one of the exceptions applies • **Principle 11 – Limits on disclosure of personal information.** Only disclose it if you've got a good reason, unless one of the exceptions applies	• The AI policy mandates staff review of outputs to ensure information sources are checked to ensure information is used for its intended purpose. • Mandatory training and terms of use (**Appendix F**) is in place to ensure users understand data sources and to reinforce correct labelling of information as appropriate. • Unintended disclosure of information or misuse of information may be managed through HR processes.	**Compliant.** Ensuring data is used for correct purpose remains a procedural responsibility supported by staff training and awareness rather than a technical enforcement.	**R-002** **R-003** **R-005** **R-006**
12	• **Principle 12 – Disclosing information outside New Zealand.** Only share information with an agency outside New Zealand if the information will be protected	• No additional overseas disclosure risks are introduced from original M365 PIA. Copilot operates in the same data environment as Microsoft 365 products, with data stored and processed in the closest available data centre (in Australian Microsoft data centres). • All information in transit is encrypted; prompts remain in tenancy and do not train the large language model.	**Compliant.** Adheres to M365 storage rules and GCDO cloud guidance.	**N/A**
13	• **Principle 13 – Unique identifiers.** Only assign unique identifiers where permitted	• Copilot does not create or rely on unique identifiers	**Compliant.** Not used.	**N/A**

12. OPC Guidance

OPC guidance recommends we consider Māori perspectives on privacy. They recommend we are proactive in how we engage. They have heard specific concerns about Māori privacy and AI tools, including:

• Concerns about bias from systems developed overseas that do not work accurately for Māori.

• Collection of Māori information without work to build relationships of trust, leading to inaccurate representation of Māori taonga that fail to uphold tapu and tikanga.

• Exclusion from processes and decisions of building and adopting AI tools that affect Māori whānau, hapū, and iwi, including use of these tools by the Crown.

Our AI Policy doesn't allow the use of AI as a proxy for cultural or translation that should be done by experts. However, we have not had a full engagement process with Māori in the preparation of our Copilot rollout, or privacy assessment. We have been awaiting more fulsome advice from GCDO/GDDA on this front. We will maintain a watching brief on this area and action any further advice as it is made available.

13. Conclusion

Microsoft 365 Copilot represents an evolution in how users interact with information already held within the Commission's Microsoft 365 environment. When implemented in alignment with existing governance, and subject to the additional safeguards identified in this assessment, Copilot does not introduce unmanageable privacy risks. This PIA, read alongside the Microsoft 365 PIA, provides assurance that the Commission's use of Copilot can proceed in a manner consistent with the Privacy Act 2020 and the expectations of the Office of the Privacy Commissioner.

14. Supplementary resources

- Public Service Commission AI Policy
- PSC AI Strategy
- AI Guidance for staff
- Acceptable use policy
- AI learning hub
- GCDO guidance: Responsible AI guidance

15. Appendices

APPENDIX A: M365 PRODUCTS WITH COPILOT FUNCTIONALITY (available from go-live)

Core Copilot surfaces	• Microsoft 365 Copilot app • Microsoft 365 Copilot Chat
Office and productivity apps	• Microsoft Word • Microsoft Excel • Microsoft PowerPoint • Microsoft Outlook • Microsoft OneNote
Collaboration and content apps	• Microsoft Teams • Microsoft Loop • Microsoft Whiteboard
Content and storage	• SharePoint Online • OneDrive for Business
Search and cross-app experiences	• Microsoft 365 Search (Copilot Search)
Platform-level integrations	• Microsoft Viva • Power Platform • Dynamics 365

APPENDIX B: SENSITIVE DATA SITES

For more information on site owners and correspondence, see the full tracking spreadsheet.

Site Name
Capability Review Programme
Governance [SSC-SPM-4]
Head of Profession [SSC-PDC-2]
Legal and Legislation [SSC-AGS-13]
Organisation Analysis [SSC-SPM-5]
Organisation Development
Public Service [SSC-CEO-2] [Includes CE recruitment]
State Sector Performance
State Sector System Design [SSC-SPM-2]
Talent Acquisition [SSC-HRM-10]
Workforce Data

HR Delivery and Operations
Reporting [SSC-HRM-9]
Personnel Files [SSC-HRM-9]
Equal Pay Taskforce
Public service reform
Pay Equity Claims
Ministerial Services
Legal and Legislation
Strategy Policy and Integrity
Leadership Development Centre
Integrity Ethics and Standards
People Team
Employment Relations Matters
Commission Investigations
Reviews
Crown Response Office
People Team
Leadership and Talent
Workforce DEI Team
Strategic Review - Finance and Efficiency
Strategic Information
Ministerial Team
Employment Relations
LDC Brokering

APPENDIX C: LIST OF SITES CURRENTLY BLOCKED FROM COPILOT REASONING AS AT 20/03/2026

Site content	Information types stored in site	Site owner
PSC inquiries and reviews	Information pertaining to system wide investigations conducted by PSC.	DCE, System, Policy and Integrity
Crown Response Office – most sensitive information site	Information held about survivors of state abuse in care	Crown Response Office
Legal Team site	Information pertaining to legal cases and other legally sensitive documents.	Chief Legal Officer

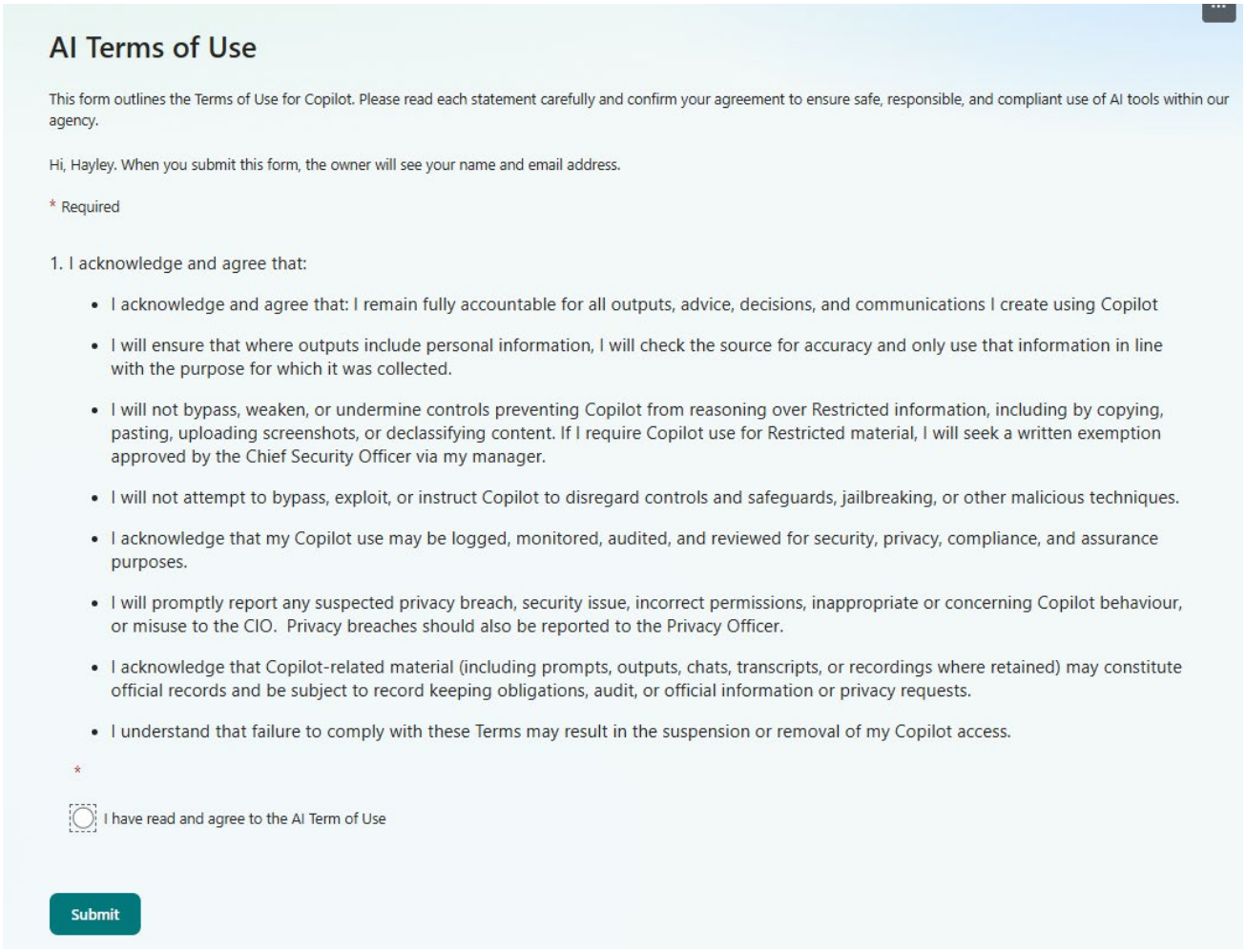
APPENDIX D: LIST OF PROPOSED CONTROLLED SITES (ONLY ABLE TO BE USED IN COPILOT BY NAMED TEAM)

Site content	Information types stored in site	Site owner
People and culture	Human resource data including sensitive staff files, recruitment, performance information etc	Chief People Officer
Legal	Sensitive legal information relating to current and past legal advice and information	Chief Legal Officer

APPENDIX E: SUMMARY OF CONTROLS – TECHNICAL AND HUMAN

Technical Controls	Human controls
A full list of technical controls can be found in the Certification and Accreditation. A summary can be found below: • Access to controlled sites is restricted using authentication mechanisms such as user IDs, passwords, and multi-factor authentication. • Data encryption is applied both at rest and in transit to protect sensitive information from unauthorised access. Audit logging and monitoring are in place to track user activity. • Regular system updates and vulnerability management are conducted to maintain the security posture of the environment.	• All staff given licenses subject to terms of use and PSC AI Policy. • Staff undergo regular training on information security, privacy, and acceptable use policies. • Sharing access to the controlled sites is limited to named team members. • Site owners are responsible for managing permissions with information management to ensuring that only authorised personnel can access or modify sensitive data. • Procedures for onboarding and offboarding ensure that access rights are reviewed and updated promptly to reflect personnel changes.

APPENDIX F: TERMS OF USE TEXT



AI Terms of Use

This form outlines the Terms of Use for Copilot. Please read each statement carefully and confirm your agreement to ensure safe, responsible, and compliant use of AI tools within our agency.

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

* Required

1. I acknowledge and agree that:

- I acknowledge and agree that: I remain fully accountable for all outputs, advice, decisions, and communications I create using Copilot
- I will ensure that where outputs include personal information, I will check the source for accuracy and only use that information in line with the purpose for which it was collected.
- I will not bypass, weaken, or undermine controls preventing Copilot from reasoning over Restricted information, including by copying, pasting, uploading screenshots, or declassifying content. If I require Copilot use for Restricted material, I will seek a written exemption approved by the Chief Security Officer via my manager.
- I will not attempt to bypass, exploit, or instruct Copilot to disregard controls and safeguards, jailbreaking, or other malicious techniques.
- I acknowledge that my Copilot use may be logged, monitored, audited, and reviewed for security, privacy, compliance, and assurance purposes.
- I will promptly report any suspected privacy breach, security issue, incorrect permissions, inappropriate or concerning Copilot behaviour, or misuse to the CIO. Privacy breaches should also be reported to the Privacy Officer.
- I acknowledge that Copilot-related material (including prompts, outputs, chats, transcripts, or recordings where retained) may constitute official records and be subject to record keeping obligations, audit, or official information or privacy requests.
- I understand that failure to comply with these Terms may result in the suspension or removal of my Copilot access.

*

I have read and agree to the AI Term of Use

Submit