

Microsoft 365 Copilot Guidance for WA Government Entities

Who is this guidance for?

This guidance supports all public sector entities in adopting the Microsoft 365 Copilot (M365 Copilot) subscription (within the Microsoft Copilot enterprise product), in line with WA Government Artificial Intelligence (AI) Policy.

What is Microsoft Copilot?

[Microsoft Copilot for Enterprise](#) is a generative AI tool which includes Microsoft 365 Copilot Chat (free for Entra account users with a Microsoft 365 subscription) as well as **Microsoft 365 CoPilot (M365 Copilot)**. It requires paid user licenses and is integrated into an organisation's Microsoft 365 environment, leveraging tools like Word, Excel, Outlook, and Teams. It uses organisational data to help staff generate content, gain insights, and improve productivity by streamlining tasks such as drafting emails, analysing information, and summarising meetings. Licensed users also have access to free in-built Copilot Agents, such as [Analyst and Researcher](#). Additional subscriptions through Microsoft Copilot Studio enable entities to build and deploy AI agents that can be used to automate business workflows without the need for further coding. The attached self-assessment has been completed for both Microsoft 365 Copilot Chat and Microsoft 365 Copilot within the Microsoft Copilot enterprise product.

How to get started with M365 Copilot?

1

Run a trial before rolling out M365 Copilot across the entity

To minimise risk understand potential productivity gains from M365 Copilot, it is recommended that public sector entities conduct an initial trial with a limited number of M365 Copilot licences to determine its value across different business areas. The trial should implement the recommendations set out in this guidance.



2 Set up correct permissions and security controls

Ensure the correct permissions are in place on SharePoint folders or sites:

Copilot only surfaces organisational data to which individual users have at least view permissions. If correct permissions are not put in place on SharePoint folders or sites, Copilot could inadvertently surface data to other users who would not normally be authorised to view that data.

Ensure adequate security protections are in place:

Protections include data remaining within the Microsoft 365 service boundary, data is not used to train large language models, data is stored and processed in Australia, and data is encrypted. While most of these measures will be enabled by default, it is important to confirm this with the vendor.

3 Ensure all users receive training

To maximise Copilot productivity gains and minimise risk, entities should consider developing Copilot training (prior to and during the trial) that incorporates the following points:

- **Exploring the full capabilities of the software:** Microsoft provides free Copilot training for all M365 Copilot license in the Viva learning platform built into the Microsoft Teams app. This is known as the *Copilot Academy*, and it is a useful training resource.
- **Ensuring proper document classification:** Staff should know to ensure that they place the proper permissions controls on documents to avoid data leaks within the organisation.
- **Ensuring human oversight:** Staff should know to always review Copilot outputs and assess for bias and accuracy. Please see the WA Government AI toolkit for public sector staff for more detailed advice on reviewing AI outputs.
- **Understanding the ‘work-web’ toggle:** when interacting with Copilot chat to understand when organisational data is used and when it is switched off.

4

Other considerations

- **Ensure your entity has appropriate AI governance processes** ([see toolkit for government entities](#)) in place to review the implementation of Copilot and investigate any issues that arise.
- **Organise a ‘Community of Practice’ Copilot discussion forum** (e.g. a Teams channel) where participants can share their use cases and communicate with the entity’s Copilot administrators.
- **Consider documenting and evaluating various Copilot use cases** and useful prompts in a prompt library.
- **Use ‘Microsoft Purview’ to audit web search queries to ensure no confidential data leaves the tenancy:** When prompts are entered into Copilot, it creates a web search query based on the user’s prompt that is sent to Bing Search Service. While only key search words are sent, and disassociated from the user ID or tenant ID, it may still include confidential data.
- **Have an incident response plan:** It is recommended that a thorough incident response plan be formulated to address any failures or misuse of the Copilot software. For example, if there are incidents that arise as a result of specific Copilot plugins or agents.

Disclaimer: It is important to understand that like many types of AI, Microsoft 365 Copilot continues to evolve as the technology is continuously subject to change. For more details on its most recent security controls, please refer to this [link](#).

Attachment 1: Microsoft 365 Copilot Framework self-assessment for WA Government Entities

AI Assurance Framework Self-Assessment

Project title:	Microsoft 365 Copilot and M365 Copilot Chat
Project description:	A WA Government Entity is looking to use Microsoft 365 Copilot Chat and acquire Microsoft 365 Copilot licences. The purpose of this acquisition is to enhance agency productivity and efficiency (e.g., summarising documents, coding assistance, streamlining document drafting, and enhancing communication. Microsoft 365 Copilot Chat is a generative AI experience that is provided as part of the existing WA Government Microsoft Enterprise Agreement. It leverages OpenAI generative AI models to provide secure, web-grounded chat capabilities, with market-leading user privacy protections and other functions including web-grounded agents, image generation, and reasoning over files. Microsoft 365 Copilot is a separately licensed add-on service to Microsoft 365. It extends the capabilities of Copilot Chat to include generative AI chat grounded on internal agency content, and a range of embedded AI functions in Microsoft 365 apps (Outlook, Word, Excel, PowerPoint, and others). It also allows for first party, third party and custom agents to be consumed/built that can integrate with existing agency systems and data, and provides other capabilities including memory, personalisation, and collaborative functions. Both solutions share the same enterprise-grade management, security, and compliance capabilities, and run within an agency's existing Microsoft 365 tenant boundary, following the same data at rest and data in transit procedures already in-place with other Microsoft 365 services used by WA Government.
What is the source of the AI solution?	Purchased or otherwise sourced from a third party.



Who are the main users of the AI tool?	Microsoft 365 Copilot Chat and Microsoft 365 Copilot are services typically used by public servants within an agency and has application to any staff member regardless of role, provided they have a use for AI-assisted web search, internal search, and productivity functions.
Which AI technology is being used?	Generative AI; Natural language processing, Computer vision, Autonomous systems and robotics, speech recognition and synthesis. Microsoft 365 Copilot and Copilot Chat are primarily based on Generative AI and NLP, however these solutions also have features that relate to Computer Vision (reasoning over images passed to it, OCR, etc) and Speech Recognition and Synthesis (transcribe speech in Teams calls and meetings, and identify voices if users have opted-in to that feature), and autonomous systems (Copilot Agents can also be configured to have autonomous action, such as being triggered by a file upload or received email).
What tasks will the AI solution primarily be used for?	Content development; Administrative workflow and process optimisation; Personalisation and user experience. M365 Copilot has broad capabilities that can align with many more than 3 choices allowed, depending on the use case/scenarios that have been identified by the participating agency, but the 3 most common tasks have been selected.

Community benefit and fairness

Government entities should be able to define and document the benefits and possible harms of the AI use case to the community, environment and entity.

What is the intended benefit of the AI solution?	Benefits for the community: Improved productivity and maximising value for money in the public service. Potentially reducing backlogs in service delivery. Benefits for the environment: There are no specific environmental benefits from our entity adopting M365 Copilot. Benefits for government: Increase our entity's efficiency and maximise value for money.
---	---



Are there potential harms posed to the community, environment and entity?	It is unlikely that the use of this tool will pose any harms to the entity, community or environment, as the appropriate security protections are in place and it does not impact decision-making. Other potential harms include: if sensitive data were to be exposed externally and misused, it could potentially be harmful to the entity and community; if outputs are not adequately verified, it could lead to a quality decline in the work of the entity, a reduction of critical thinking skills among entity staff and a decline in trust from the public.
What stakeholder groups may be impacted by the AI system, and how?	Entity employees: Positive impacts: Increased Efficiency: Enhancing efficiency of administrative tasks allows employees to focus on more strategic and impactful work. Skill Development: Working with Copilot could enhance AI information and communication technology (ICT) skills. Negative impacts: Potential overreliance on AI leading to a decline in quality of work. The need to overcome a learning-curve to effectively use the technology. Agency senior stakeholders (management, ED, DG level): should see a cumulative impact from productivity and efficiency gains from broad adoption of Copilot. These stakeholders will need to allocate budget and effort for the governance and management of the solution, as well as end-user training. ICT department: Increased workload: ICT employees will need to train staff to use Copilot safely and effectively. Citizens: Positive impacts: Improved Services: Faster and more accurate responses to inquiries, applications, and service requests, leading to higher citizen satisfaction.



Privacy, security, transparency, explainability and contestability

AI solutions must be well understood, documented, explainable and contestable. This is crucial to making AI use transparent and fair.

Please provide information that is currently available to you or indicate what is planned.

What data does the AI solution use to function, test, train, and validate? Indicate whether the data reflects the population or environment that will be impacted by your project or service?	Microsoft 365 Copilot is underpinned by large language models (LLMs) from Microsoft and Open AI, which are pretrained on publicly accessible data that has been cleansed and curated. Data informing Copilot's outputs may contain bias. It is not reflective of the population. These models are grounded on both web search (if enabled by the agency and/or user) using data from the internet and organisational data from the Microsoft Graph (in the case of Microsoft 365 Copilot) including email, chat messages, calendar, meeting transcripts, SharePoint documents etc that users have existing permission to access. This may include unofficial to official-sensitive information. Microsoft does not use the entity's data to train the generative AI models underpinning Microsoft 365 Copilot and Copilot Chat and has contractual commitments to protect user privacy and not allow tracking or advertisement when using Copilot to perform web queries.
How is the data for your project handled?	As with other Microsoft 365 services in use by WA government agencies, Microsoft 365 Copilot and Copilot Chat data is stored at rest in local data centres within Australia. As with all Microsoft 365 services, Microsoft may process data requests in other locations if necessary to ensure optimal performance and service availability. Data processed as part of interactions with M365 Copilot and Copilot Chat are fully encrypted in transit and at rest (using TLS 1.2 and AES-256) and agencies can utilise Customer Managed Keys for additional surety. Microsoft 365 Copilot queries sent to the Large Language Model are stateless.



	The information contained within Copilot prompts, the data they retrieve, and the generated responses remain within the Microsoft 365 service boundary. Microsoft 365 Copilot and Copilot Chat are both covered by the Microsoft Enterprise Agreement, Microsoft Product Terms, Copyright Commitment and Microsoft Enterprise Data Protection, which defines data processing and handling, data security, privacy, and other data protection commitments related to these solutions. Enterprise data protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat Microsoft Learn
What are the intended AI data outputs?	Examples of outputs include: email drafts, policy drafts, document summaries, internal meeting minutes and data analyses.
How does the AI system generate these data outputs?	Copilot generates outputs by connecting organisational data to LLMs. 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 in the user's tenant. • Grounding improves the specificity of the prompt and helps generate answers that are relevant and actionable to the 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. 3. Copilot sends the grounded prompt to the 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.
How will AI outputs be monitored and reviewed over the lifecycle of the project?	All interactions with Microsoft 365 Copilot and Copilot Chat can be audited, monitored, and reviewed through the Microsoft Purview capabilities that are part of the current WA Government Microsoft Enterprise Agreement.



	This includes a detailed audit log of interaction with the technology, including prompts and responses. Purview eDiscovery has scope of this information for broader compliance and investigation. Policy-based monitoring is possible through Purview Communications Compliance and Insider Risk Management, proactively notifying agency administrators when use of this technology is in violation of acceptable use policies, or indicates a potentially malicious action. Additionally, Copilot Analytics provides comprehensive usage reports and insights through the Copilot Dashboard and Viva Insights. All of these capabilities are agency configurable and are part of the current WA Government Microsoft Enterprise Agreement. Every 6 months, any changes or updates to Microsoft 365 Copilot will be reviewed by the AI Accountable Officer and relevant AI governance group.
The WA Government AI Policy requires the community to have access to an efficient review mechanism about AI-informed outcomes that impact or engage with them. Has the use of AI been (or will it be) disclosed to all users or significantly impacted parties?	☐ N/A Provide rationale: AI will not be used in decision-making, and staff will be trained to provide appropriate oversight when reviewing generated content. There will be no public users interacting directly with the AI.



Controls

All AI projects should have appropriate controls in place to ensure outputs are safe, secure and reliable.

Please indicate which of the following controls have been, or are planned to be, incorporated in your project. Please briefly describe how each control will be **applied** and **document limitations**.

AI outputs are subject to human validation.	Communications will be provided to staff around expectations for how they should use the tool. It will be made clear to users that all outputs from Copilot must be reviewed for accuracy and bias. User training will also support this objective. Copilot provides citations for all sources it has used to generate its output. Users can these citations both inline and referenced beneath each response. Limitations: if users forget to review or over rely on outputs.
Training for public sector users of AI.	Users will have to undertake mandatory training. The pilot users will go through an initial training orientation before they can use the license. There will be regular group meetings and a Teams site created to support each other with issues. Each M365 Copilot user will gain access to the Microsoft Copilot Training Academy which has units on the ethical use of AI, how to generate prompts, in addition to use within each application. Microsoft also provides supplementary training on its use, content generation, search, and using it within each of the Office apps. There is also WA government-specific training through programs such as the Snackable Series and the Enterprise Skills Initiative (ESI). Viva Insights provided organisation and group level metrics on the uptake and impact of Copilot usage. Review of these metrics can inform targeted training initiatives to uplift capability in using Microsoft Copilot. Limitations: none.



Impacted stakeholders are consulted.	Senior executive staff will be consulted to identify users. There will be monthly meetings of the entity’s AI working group to discuss reported issues/progress concerning AI. Additionally, there will be a bimonthly meeting between the AI working group and the executive to update them on AI progress including Copilot implementation. We will set up a community of practice for the group to collaborate and share experiences and use cases. Regular reviews with users will be held to verify user feedback and productivity gains. Limitations: none.
AI systems are subject to regular reviews and audits for accuracy, fairness, and bias.	Users will be made aware of issues that AI may have with accuracy, fairness and bias during their AI training. Users will report any issues they come across to the AI governance group who meets monthly to discuss the implementation of AI. Microsoft Purview will be used to ensure web search queries do not contain any OFFICIAL Sensitive data. Limitations: none.
An incident response plan is in place to address potential AI system failures or misuse.	The entity’s AI governance group will investigate incidents concerning Copilot. If there are incidents that arise as a result of specific Copilot plugins, the entity is prepared to disable these plugins until further notice.



	If incidents arise due to Copilot itself, the entity is prepared to temporarily or permanently disengage from the software. Microsoft provides a suite of services for Security Oversight of Copilot to tackle misuse. Limitations: none.
--	---

The team is prepared to disengage the AI system if an unresolvable problem is identified.	If any issues are flagged throughout the project, the simple solution will be to remove the licenses from the selected group.
---	--



Requirements

Your AI use case must comply with:

- The [WA Government AI Policy](#), and any further policy requirements expected by your entity.
- The [WA Government data offshoring position and guidance](#).
- Privacy requirements under the [Privacy and Responsible Information Sharing Act 2024](#) (WA).
- Cyber security requirements under the [WA Government Cyber Security Policy](#).
- Australian [anti-discrimination laws](#).
- Record keeping requirements under the [State Records Act 2000](#) (WA) and [Artificial Intelligence and Record Keeping guidance](#).
- Other relevant laws and policies

☒ Yes, I confirm that this project / AI use case complies with the above legal and policy requirements.

Note that legal advice should be sought where there are necessary compliance concerns, including when sensitive data is used by the AI system.

Risk assessment

Step 1: Some applications of AI are considered to be high risk in nature, requiring oversight by the Board. Will the AI use case involve or impact any of the following?

- ☐ Biometric systems, including for identification and emotion recognition purposes
- ☐ Educational or vocational training that may be used to determine access to institutions or evaluate learning outcomes
- ☐ Law enforcement and administration of justice which may impact someone's livelihood
- ☐ Employment, personnel management and access to self-employment (including recruitment, contracts and performance evaluation)
- ☐ Safety components in the management and operation of critical infrastructure (including digital, transport, water, energy etc.)
Access to essential private and public services (including assistance benefits, healthcare services, and emergency responses)

☐ None of the above

Step 2: Procuring AI software or involving a third-party may expose your use case to high privacy and security risks because of where the information is stored.

Will the AI use case use OFFICIAL Sensitive government information?



☐ Yes, and information is **hosted** or processed **offshore** (Note: this will require you to demonstrate evidence of special security controls to the AI Advisory Board)

☐ Yes, but information is **hosted** and **processed in Australia**

☐ No

Note that the risk of offshoring non-sensitive personal information and official government information should also be considered and mitigated through security controls per the [WA Government data offshoring position and guidance](#).

Microsoft ensures that M365 Copilot and Copilot Chat data will be stored with the agency's M365 tenant in Australia. No data will be hosted offshore. Microsoft 365 Copilot has been independently assessed against IRAP PROTECTED standards in 2024, with the full 157-page report (Microsoft 365 - Security Fundamentals and Cloud Services IRAP Assessment Report (2024)) published on the Microsoft Service Trust Portal (<https://servicetrust.microsoft.com/>). Calls to the underlying LLMs (generative AI models) will be made locally, however as with other Microsoft 365 services, Microsoft may route calls to other regions for performance and service availability reasons. Any transfer of information in this process is fully encrypted using TLS 1.2 and agencies have the option of using Customer Managed Keys for extra surety.

Step 3: Please complete the below risk assessment in consideration of your previous responses and planned controls. Note that controls can only mitigate, but do not resolve all risks.

Assess the following residual risks:

	N/A	Low	Medium	High
Community benefit and fairness				
Potential discrimination, bias or disproportionate impact on a specific community.		X		
Potential harms to an individual, community or the environment. This includes physical safety, as well as breaches to an individual's rights, privileges and entitlements.		X		

Provide a rationale: Users will be trained to apply human oversight on all AI outputs, therefore these risks will be low. Microsoft 365 Copilot and Copilot Chat have an internal content safety system, to mitigate the risk of inappropriate use or content generation. This is built in alignment with [Microsoft's Responsible AI principles](#).

Influencing harmful decision-making or service outcomes



Overreliance on AI outputs in government decision-making, service delivery or business processes.		X		
Inaccurate or poor quality data inputs to the AI model, thus influencing government decision-making, service delivery or business processes.		X		

Provide a rationale: Users will be trained to apply human oversight which will mitigate overreliance and poor outputs. AI will not be used in decision making.

Privacy and security

Personal or sensitive government information being misused or inappropriately collected (consider the involvement of third parties).		X		
The AI system or use case posing reputational risks or undermining public confidence in government.		X		
The AI system or use case raising security concerns due to the sensitivity or classification of the data used, and where the data is stored (i.e. inside Australia versus offshored as indicated in step 2).		X		

Provide a rationale: The security measures in place ensure that Microsoft will not use the entity's data to train its models, and the data will be stored in Australia. Reputational risk will be minimised by training users to apply human oversight on all outputs. M365 Copilot acknowledges content sensitivity through its processes, and any output which aggregates data of differing sensitivity levels will inherit the highest sensitivity level of that data collection.