

How to Use Artificial Intelligence Safely

Interim Guidelines

May 2026 | Version 2.1 (Public facing for DOJ website)



Contents

Contents	2
How to use Artificial Intelligence (AI) safely	3
What is the Agency's recommended generative AI tool?	3
Use of other AI tools	4
Other generative AI tools	4
Embedded AI	4
Agentic AI tools	4
Keep Personal Information Safe	4
Keep Organisational Information Safe	5
Be Clear and Transparent	6
You're in Charge, Not the AI	6
For Output Managers and Team Leaders	7
Final Considerations	7
Related Information	7
Definitions	8
Examples of safe and responsible use of AI	8
Helping to find a venue for an event	9
Help with a simple data analysis	9
Summarising a report	10
Taking notes for a meeting	10
Drafting an email	11
Taking a group photo	12
Analysing responses to a request for tender	12
Policy Details	13

Summary

These interim guidelines provide immediate direction to Department of Justice staff on the use of artificial intelligence and will be replaced by a formal Agency policy once it is finalised.

Use of unapproved software is prohibited under the Department's Acceptable Use of ICT resources policy.

The only general-purpose artificial intelligence tool approved for use within the Department is Microsoft Copilot.

How to use Artificial Intelligence (AI) safely

AI tools are changing the way we all work. Whether it is helping us draft new content, rewrite, or summarise documents, analysing data or aiding us in research.

Many types of AI tools exist. Some of the more commonly used types are:

- Generative AI tools such as ChatGPT, Microsoft Copilot Chat and Claude
- Embedded AI and AI assistants in commercial products: AI tools that work within existing software platforms to augment the work staff do within that platform. For example, Microsoft Copilot embedded AI assistants in the web-based versions of Office products.
- AI Agents or AI tools developed or trained for a specific purpose: a tool that uses AI to perceive information, make decisions and take actions toward defined objectives using human defined controls and oversight. Some chatbots are examples of this.
- Agentic AI tools: designed to autonomously or semi-autonomously plan, initiate and execute sequences of actions to achieve defined objectives rather than relying on individual human instructions.

Whilst the opportunities for AI are promising, they can also involve risk, particularly for governments.

This guide has been developed to support staff to use these tools safely, effectively, and responsibly. This is interim advice to provide guidance until the release of the formal State Government and Agency policies, which is expected in the coming months.

What is the Agency's recommended generative AI tool?

The Department's preferred generative AI tool is Microsoft Copilot Chat which can be accessed from the Microsoft Edge  web browser and from within the web version

of Microsoft Office products such as Teams, Outlook, Word. Copilot Chat (the  icon is found in the top right-hand corner of Edge) works in a way that should prevent Agency information from leaving our Microsoft 365 environment (enterprise data protection), so that any uploaded documents will not be accessible outside of the Department of Justice.

Copilot Chat is the entry level Microsoft AI tool and is available to all Department of Justice staff. It is a chat-based AI tool (similar to Chat GPT) and references public web data and specific files that you upload. It does not access organisational emails, Teams chats or documents.

Use of other AI tools

Other generative AI tools

The use of other generative AI tools (such as Chat GPT, Claude, Gemini) beyond Copilot Chat is not authorised due to the risks they pose to potentially sensitive Government information leaking into the public domain or incorrect/inaccurate information being relied upon for business decision making or advice to Government.

If staff wish to use other tools, a software request must be submitted that will be reviewed by the office of the Chief Information Officer (OCIO)t, which will assess safety and security.

Use of Deep Seek is prohibited in all circumstances.

Embedded AI

Microsoft Copilot assistants that are embedded within Office products also use enterprise data protection (any data is kept within our organisation).

Many software platforms are offering embedded AI, usually as a licenced additional feature. Every implementation of an AI tool is different, and the risks need to be assessed individually. If staff are interested in an AI feature offered for a software package, a software request can be submitted to start the assessment process, which will include a review of safety and security.

Agentic AI tools

Until further notice, Agentic AI tools are currently not allowed at the Department because they raise concerns around accountability, security, and compliance, as autonomous decision making without sufficient human oversight could cause the Department reputational damage.

Keep Personally Identifiable Information Safe

The information in this section is important when using AI tools that are not covered by enterprise data protection (any tool that is not Microsoft Copilot).

When using AI tools, staff must always protect people's personal details. Make sure these details can't be traced back to the person they belong to (e.g. don't include personal information in the prompt).

What is Personal Information?

It is any detail that could be used to identify, impersonate or track someone online.

Do not use personal information

When using AI chatbots or other tools that do not have enterprise data protection (such as Chat GPT), always:

- **Change Details:** Change personal details so they can't be traced back to a person.
- **Hide Real Details:** Swap out real details, like emails or phone numbers, with made-up ones.
- **Use Only What's Needed:** Only use the details that are relevant.
- **Check the Settings:** Check the privacy settings to make sure data is not stored or used to further develop (train) the system. This keeps sensitive information safe and prevents it from being shared with others using the service.

Keep Organisational Information Safe

The information in this section is important when using AI tools that are not covered by enterprise data protection (any tool that is not Microsoft Copilot).

When using AI tools, always protect the Agency's confidential data, particularly the personal.

What is Organisational Information?

It refers to any data or detail that can identify or provide insights about the Department. This includes operational data, financial records, business strategies, and employee data. Ensure that these details cannot be used maliciously.

How to Protect Organisational Information?

If using an AI tool that does not have enterprise data protection:

- **Anonymise Data:** Modify organisational details so it can't be traced back to the organisation.
- **Substitute Real Data:** Replace genuine details, like business emails or contract numbers, with fictitious ones.

- **Limit Data Exposure:** Only use the data that is essential for the task at hand.
- **Review Privacy Controls:** Regularly check the AI tool's privacy settings to ensure that organisational data is not stored or used to 'train' the system. This preserves the confidentiality of the data and prevents it from being accessed by unauthorised users or other entities using the service.
- **Ask yourself, "Is the Information Sensitive?":** Consider the nature of the content, would it be detrimental to the Agency if the information was to be made public independent of official channels.

Be Clear and Transparent

Sometimes, AI tools might give information that's not 100% correct or might be biased. It should also be clear when AI tools are being used by government to inform activities. Staff should consider including markings in briefings and official communications indicating if AI was used to generate any of the information.

Always:

- Check where the information came from, ask the AI to provide a source.
- Be ready to explain any advice or choices produced by the AI.
- Triple-check AI's answers to make sure they are right and useful.

You're in Charge, Not the AI

AI tools are helpful, but they don't think for us. Staff need to make sure what they generate is in line with the Department's Values and Strategic Plan.

- **Check AI's Work:** Staff need to make sure that what the AI writes or suggests is right and fits the intended goals.
- **Tell AI Clearly What You Want:** To get the best out of AI, give clear prompts, instructions, and examples.
- **Keep Learning:** It is important that staff keep learning, especially about online safety, protecting data, and using AI in a considered way.
- **Be Open:** Acknowledge and label content that has been partly or wholly generated using AI.
- **Don't allow AI to make final decisions:** AI use in the Tasmanian Government must be transparent and explainable to the public. It is important that staff can explain, justify and take ownership of advice and decisions that involve AI.

For Output Managers and Team Leaders

Managers have an important role in making sure they are aware if their staff are using AI tools in their work:

- **Be Clear:** Decide whether it is reasonable for staff to use AI in their work.
- **Promote Safe Use:** Remind team members to use AI in a transparent and ethical way.
- **Review How AI is Used:** Make sure their team uses AI the right way through regular reviews.
- **Talk Openly:** Let team members talk about any AI questions or worries they have.
- **Stay Updated:** As AI changes, making sure thier team's ways of using it change too.
- **Encourage your team to learn and experiment safely**

Final Considerations

AI is an emerging technology, and the Office of the Chief Information Officer (OCIO) will regularly review these guidelines to ensure they remain relevant and reflect the available tools and services.

An AI Working Group has been established to progress policies, strategy and training for staff.

These are general guidelines, and it may be inappropriate for some uses of AI for specific work or field of practice. Staff should always speak to their manager before using AI in their work.

If staff feel unsure they are using AI tools safely and would like further advice, they can contact the service desk.

Related Policies

- Department of Justice Acceptable Use of ICT Resources Policy
- Department of Justice Information Security Policy
- [Tasmanian Government Personal Information Protection Policy](#)
- [Australian Government policy for the responsible use of AI](#)

Definitions

Artificial Intelligence (AI): is an umbrella term for a range of technologies that enable computers to mimic human capabilities, particularly in the areas of problem-solving, planning, natural language processing, computer vision and more. These systems can improve their performance over time.

Examples

- Microsoft Copilot Chat
- OpenAI ChatGPT
- Google Gemini
- Meta AI (Facebook)
- Anthropic Claude
- Perplexity AI
- Grok
- Cohere

Generative AI: Generates new content such as text, images, code or even music. This content contains characteristics similar to that found in human generated content by using models to find patterns and structures in the data it is trained on. An example of generative AI are ChatBots that produce human like responses or create imagery from text.

Large Language Models: These are tools that use deep learning to make text that sounds human. They learn from lots of texts to understand how language works. They can answer tricky questions and give long, helpful answers. They also understand computer programming languages. This means they can help write code, find mistakes in code, and give ideas to make code better.

Examples of safe and responsible use of AI

This section provides example uses for Generative AI tools. These are a guide only. They are not intended to be an exhaustive list of applications and should not be taken as an endorsement of specific tools or uses. The appropriateness of each use is based on individual circumstances, and the nature of the content and information being used. If in doubt, please consult with your manager or the service desk.

These have been adapted from the [Guidance for the safe and responsible use of Generative AI in the Victorian Public Sector](#)

Helping to find a venue for an event

The situation	Gen AI use case	Appropriate use?
You have booked a venue for community consultation workshops which members of the public have nominated to attend, but with just one week to go the venue has cancelled your booking. You need to quickly book an alternative venue for your workshop.	You ask the publicly-available Generative AI tool to provide you with a list of venues including contact details, capacity, average price and customer reviews. You call the top three venues recommended by the Generative AI tool to confirm cost and availability before making a booking.	Yes. You used Generative AI to find and summarise publicly-available information. You called the venue to confirm the information was correct before acting on the Generative AI tool's recommendations. Additional consideration If the event being held was confidential or had specific security requirements, event details should not be entered into a publicly available Generative AI tool.

Help with a simple data analysis

The situation	Gen AI use case	Appropriate use?
You are putting together a spreadsheet and would like to analyse the data. The data in the spreadsheet relates to a project you are working on. The data does not include personal, sensitive or health information. Your organisation has an agency-approved Generative AI tool that can be used for official work	You ask the Generative AI tool to analyse the data and provide any relevant insights. You review the analysis provided by the tool to ensure it is working as intended.	Yes. Your use complies with the tool's permitted purpose and does not contain any content or information that cannot be used in the tool. You reviewed and validated the output of the Generative AI tool before using it.

purposes where no personal, sensitive or health information is present.

Don't forget to label the analysis as being created by Generative AI.

Summarising a report

The situation	Gen AI use case	Appropriate use?
A reputable thinktank has just officially released a 500-page report on a topic you are presenting to colleagues next week. You have an incredibly busy week full of other deadlines and will not have the opportunity to read the full 500-page document and update your presentation.	You use a Generative AI tool to summarise key findings of the report and provide you with the references to the pages on which they appear. You review sections of the report that the Generative AI tool has referenced to confirm the summaries provided are accurate. When you give the presentation, you disclose that the summary was generated by Generative AI. You advise your audience to review the report and to not rely on the summary provided by Generative AI.	Yes. The information in the report is public information. You are an expert on the topic so can identify incongruent information if it exists. You also validated the summary back against relevant sections of the report to ensure it accurately reflects the content of the report. You labelled the summary as being created by Generative AI.

Taking notes for a meeting

The situation	Gen AI use case	Appropriate use?
---------------	-----------------	------------------

You are hosting an online meeting with your team to discuss a work project. The online meeting software you are using has been approved by your organisation for official work purposes. You need to take minutes for the meeting but there is no one in your team available to help.	You use a feature in the online meeting software to record the meeting and take notes. The software says that the feature is powered by Generative AI, so you ask everyone's permission to turn on the feature. You remind everyone in the meeting not to discuss any sensitive topics.	Yes. The Generative AI tool has been approved by your organisation for use, and you asked everyone's permission first before using it. Don't forget to disclose to your team that you are recording the meeting. Don't forget to turn off the Generative AI tool if someone no longer consents to the recording. Don't forget to review the Generative AI tool's meeting notes to ensure they are accurate. If you're not sure, review the recording of the meeting. Don't forget to review access to the meeting to ensure that only those who require them have access.
---	--	---

Drafting an email

The situation	Gen AI use case	Appropriate use?
You receive an email from a difficult stakeholder with which you have been discussing a sensitive matter. You wish to respond in a firm yet polite way, but you are not sure how to do it.	You copy and paste the email chain into a Generative AI tool and ask it to draft a response for you.	If you are using a Gen AI tool other than Microsoft Copilot - No. The information you provided to the Generative AI tool is sensitive and not publicly available. The tool may inappropriately share this information with other users.

		If you are using Microsoft Copilot - Yes. As we have enterprise data protection enabled for Copilot this will ensure that the sensitive stakeholder data will not be shared.
--	--	---

Taking a group photo

The situation	Gen AI use case	Appropriate use?
You have organised the department's executive board strategic planning retreat. At the end of the last day the participants gather for a group photo to commemorate the occasion. Several executives had to leave earlier in the day, but you have access to their profile photos.	You upload the group photo and the absent executive's individual photos into a Generative tool and ask it to produce a group photo that includes all participants. You use the photo for an all-staff email about the event.	No. The photo is a record of the event, and it is not consistent with the Tasmanian State Service Principles to knowingly produce an incorrect record. It may also be a breach of privacy to use someone's photo without their consent.

Analysing responses to a request for tender

The situation	Gen AI use case	Appropriate use?
You are on a procurement panel and been provided with several lengthy responses from vendors that detail their proposals, pricing and associated service catalogues. You have been asked to analyse the proposals and rank the proposal	You upload all the documents to a publicly available Generative AI tool and ask for them to be compared and a report generated with a summary and rank for each proposal.	No. Not only do the proposal documents contain confidential information, you also have no way of explaining how the offers were compared and how the Generative AI tool arrived at the ranking for each vendor. It is also unlikely that existing Tasmanian Government procurement and policies

to determine the best offer.

would have been adequately applied.

Policy Details

Responsible Officer	Chief Information Officer
Responsible Branch	Chief Information Officer
Date approved	11 May 2026
Review date	21 September 2026
Reference	DOC/24/17949
Version	2.1