



Guidance on the use of generative artificial intelligence (AI)

March 2026

This guidance outlines the responsibilities of all Department of Finance (Finance) staff, including contractors, when using generative artificial intelligence (AI) tools in their work.

Staff must follow this guidance when using any generative AI tools. This includes:

- Microsoft 365 Copilot chat
- Microsoft 365 Copilot (Full licence)
- Public generative AI technologies (e.g. ChatGPT, Claude or Gemini)

AI tools offer significant opportunities to improve productivity and service delivery within the department, but also carry risks that must be understood and managed appropriately. Staff should ensure their use of AI tools is consistent with Finance's [AI Transparency Statement](#), [Australia's AI Ethics Principles](#) and [APS Values](#).

Where should you start your AI journey?

To begin your AI journey, follow this structured three-step process designed to build foundational knowledge, practical skills and alignment with policy, guidance and best practice.

As a first step, staff planning to use AI tools **must** complete the APS Academy's [AI in government fundamentals course](#). This foundational training helps staff understand the capabilities, limitations and ethical considerations of AI use in government. Further information on using AI safely and responsibly is available on AI for Finance's [Intranet page](#) and in the monthly [AI Newsletters](#).

As a second step, staff are encouraged to build prompting skills in a secure environment using the GovAI's [Interactive Learning Environment](#). GovAI provides a safe space to experiment with AI tools and learn effective prompting techniques without risking exposure of personal or sensitive information.

As a third step, staff should speak with their managers about how this guidance applies to their role, responsibilities and business area, including whether they should request a full Copilot licence. These conversations should clarify which tasks must not be performed using AI tools and identify the team's approved AI use cases.

Staff can view their team's approved AI use cases and supporting documentation in Finance's AI Use Case Register, available through the [AI for Finance Action Hub](#).

To request a Copilot licence, submit a request through the [Self Service Portal](#). Before completing the form, please review the guidance on [Requesting a full licence to Microsoft 365 Copilot full licence](#).

OFFICIAL

What is the acceptable use of AI tools in Finance?

Staff must use generative AI tools safely, responsibly and ethically in line with departmental policies and APS values. This includes respecting data classification, legal obligations (including privacy) and ensuring human oversight in all decision-making processes.

Do be safe, responsible and ethical

- **Use AI to support, not replace, human judgement**
People bring integrity and ethical decision-making to their work, which is why final decisions must always be made by people—not AI. When using AI, apply your [APS Values](#) and follow [Australia's AI Ethics Principles](#).
- **Keep it safe, reliable and secure**
Confirm the accuracy, security and reliability of your prompt or AI solution before use. Apply appropriate assurance measures and risk controls. Ensure personal, protected and classified information is not used with unregistered AI use cases, especially AI use cases that involve [public generative AI tools](#) in line with the [Protective Security Policy Framework](#).
- **Respect personal privacy**
Safeguard personal information against misuse, loss and unauthorised access. Comply with the [Privacy Act 1988](#), including the [Australian Privacy Principles](#) and follow the Finance's [Privacy Policy](#). Understand what personal information is in records accessed by AI and before use, confirm individuals have received privacy notices explaining that Finance may use AI in relation to their information.
- **Be transparent and explainable**
Consider whether you need to disclose AI use (it's not always required). If disclosure is needed, follow the National Archives of Australia's [Guidance on managing records created using AI](#). Always be ready to explain how AI works in clear, plain language, consistent with [Australia's AI Ethics Principles](#).
- **Stay accountable**
Ensure AI-generated content is always subject to human oversight and clear accountability. Define roles and responsibilities for using AI so staff understand what's expected. This promotes safe, ethical practices aligned with [Australia's AI Ethics Principles](#) and the [APS Values](#).
- **Use AI for good**
AI should be used to benefit society. Consider fairness, human dignity and inclusion from the start, consistent with [Australia's AI Ethics Principles](#).

OFFICIAL

Don't cut corners

- **Don't use AI without training**
Staff intending to use AI tools must complete the APS Academy's [AI in government fundamentals course](#). Managers should also provide supplementary training to ensure staff understand how this guidance applies to specific roles, tasks and business functions.
- **Don't rely on AI to make decisions**
AI should never be used to make decisions, especially those that could affect someone's rights, safety or wellbeing without proper human oversight. Always make sure a human is responsible for the final decision.
- **Don't assume AI is always right**
AI can get things wrong or produce results that don't make sense. Always apply human judgement, verify outputs and challenge results. Review all AI outputs, and if something seems off, seek a second opinion or escalate.
- **Don't ignore ethical risks**
Monitor your AI solutions for unfair outcomes, opaque logic, data quality issues, model drift, privacy breaches or security weaknesses. Raise concerns early, seek advice and document how they are addressed.
- **Don't mishandle personal or sensitive information**
Only handle personal information consistently with the [Privacy Act 1988](#) including applying the [Australian Privacy Principles](#) and the [Protective Security Policy Framework](#) for classification, protective markings and secure handling.
- **Don't assume all AI use is approved**
Before using AI with personal, protected or classified information, consult your supervisor. If no prior approval exists, register a use case in Finance's [AI Use Case Register](#). Registration ensures your AI use complies with laws, regulations and policies.

Who to contact for further guidance, policy advice or incident management:

- **General AI enquiries:** Please contact the AI for Finance team (s22 [REDACTED]).
- **AI Procurement:** Please contact ICTD Frontdoor (s22 [REDACTED]).
- **Security concerns or incidents:** Please contact the Information Technology Security Advisor (s22 [REDACTED]).
- **Privacy advice or incidents:** For privacy advice and to report any privacy breaches, contact the Privacy Team at Privacy@finance.gov.au or using the [Data \(Privacy\) Breach Incident Reporting Form](#)

OFFICIAL

What information can you use with AI tools?

Staff must ensure that any information or data entered into AI tools complies with the [Protective Security Policy Framework](#), [Privacy Act 1988](#) and Finance’s [Privacy Policy](#). This includes understanding what types of information can and cannot be entered into each AI tool. The rules vary depending which AI tool you are using.

Public Generative AI

AI tools such as ChatGPT, Gemini, Claude are external platforms not deployed within Finance’s ICT environment. Staff may use up to official: unclassified information with these tools, but must not input personal, protected or sensitive information.

Further information on what may or may not be used with public generative AI tools is available in the Digital Transformation Agency’s [staff guidance on public generative AI](#).

Copilot Chat

A general AI tool available to all staff. It operates in “web mode,” meaning it uses publicly available information from the internet to complete tasks. It can be used with up to official information, but must not be used with personal, protected or sensitive information.

Copilot (Full licence)

Finance’s enterprise-grade AI tool deployed securely within our ICT environment, also known as ‘Work mode’. It enables advanced business efficiency AI use cases that require the use of protected information, including the creation of lightweight AI agents. Further information on the difference between ‘Web Mode’ and ‘Work mode’ can be found in the [Microsoft 365 Copilot: Work vs Web Explained](#).

If seeking to use personal information when using Copilot (Full licence), you will need to complete a Privacy Impact Threshold Assessment (PITA) and consult with the Privacy Team. Read more about a [Privacy Impact Threshold Assessment](#).

The table below outlines what information types are permitted across different AI tools.

AI Tool	Permitted Information	Do Not Enter
Public Generative AI Tools	<ul style="list-style-type: none"> – Unofficial – Official: unclassified 	<ul style="list-style-type: none"> – Personal – Sensitive – Classified – Protected
Copilot Chat & Copilot (Full licence) ‘Web Mode’	<ul style="list-style-type: none"> – Unofficial – Official (non-sensitive) 	<ul style="list-style-type: none"> – Personal – Sensitive – Classified – Protected
Copilot (Full licence) ‘Work Mode’	<ul style="list-style-type: none"> – Unofficial – Official – Sensitive (AI use case required) – Protected (AI use case required) 	<ul style="list-style-type: none"> – Personal (unless a PITA has been completed)

Note: Further information and guidance on information classification, including definitions, can be found in the [Protective Security Policy Framework](#).

OFFICIAL

When and how to register your AI use case

What is an AI use case?

An AI use case is a clear example of how AI can be used to help with a specific task at work. For instance, AI might be used to write reports, answer questions, or summarise documents. It's different from a business case. A business case explains why a project should be funded. An AI use case focuses on how AI is actually used in a real situation to solve a problem or improve a process.

Further information and examples of AI use cases within government is available in [APS AI Use Case Library](#) on GovAI.

How to register an AI use case?

Submit your AI use case through the [AI Finance Action Hub](#). When completing the form, you must attach either:

- a [Simple AI Risk Self-Assessment](#), or
- a [Complex AI Risk Self-Assessment](#).

When to register an AI use case?

Registration ensures each use case is reviewed for alignment with Finance's approach to adopting AI across the department.

For further information, including which *AI Risk Self-Assessment* is required for your use case, visit the [When to register or update an AI use case](#) intranet page.

The table below provides a quick reference guide on when registration of an AI use case is required.

Type of Information Used	Copilot	Other No-Cost AI Tools	Paid AI Tools or Systems
Unofficial	No registration needed	No registration needed	Consultation required Please contact ICT Front Door
Official: Unclassified	No registration needed	No registration needed	Consultation required Please contact ICT Front Door
Official	No registration needed	Not approved These AI tools are not approved for use with this information.	Approval required Please contact ICT Front Door
Personal, Sensitive, Classified or Protected	Registration required Please register an AI use case	Not approved These AI tools are not approved for use with this information.	Approval required Please contact ICT Front Door

Procurement of AI tools or systems

Staff who want to procure an AI tool or system, including a paid subscriptions must first contact the ICTD Front Door at s22

OFFICIAL

When to disclose the use of AI in your work

Staff should apply sound judgment when deciding whether to disclose the use of AI in their work, in line with the National Archives of Australia's [Guidance on managing records created using AI](#).

Disclosure is not required when:

- AI is used for routine drafting or summarising, and the final content is reviewed and approved by a staff member.
- The content is low-risk, administrative or internal and does not influence decisions or public communications.
- The content is clearly marked as a draft and will undergo substantive editing before use.

Staff must disclose the use of AI when:

- AI-generated content significantly influences decision-making, including policy, advice or operational outcomes.
- The content could reasonably be mistaken for human-generated, particularly when it references real people, places or events.
- The content has not been reviewed by a subject matter expert.
- Legal or ethical obligations require disclosure.

How is AI governed in Finance?

Finance is committed to the safe and responsible use of AI. We consider AI offers significant opportunities to improve productivity and service delivery within our workplace.

We have an AI Governance Committee (AIGC) to oversee our adoption and use of AI within Finance. The functions of the AIGC include:

- define and promote a vision and strategy for AI that supports the mission and values of the department
- ensure the safe and controlled development and implementation of AI within Finance
- provide guidance and recommendations on the ethical, legal, and social issues and responsibilities with respect to the use of AI in the department
- ensure Finance adheres to all relevant Whole of Government legislation, regulation and industry standards in relation to the use of AI.

The AI for Finance team acts as the secretariate for the AIGC. To table an item for discussion or to contact the Committee, please contact the secretariate by emailing [s22](#).

If you would like learn more about Finance's approach to AI, please view Finance's [AI Transparency Statement](#).

OFFICIAL

Whole of Australian Government AI policy

To ensure safe and responsible use, Finance governs AI in line with laws, regulations, the Digital Transformation Agency's (DTA) [Policy for the responsible use of AI in government](#) and best practice.

We apply guidance set out in DTA's Pilot [Australian Government AI assurance framework](#) and have limited our use of AI to low-risk use cases. This guidance implements [Australia's AI Ethics Principles](#) and uses the [Organisation for Economic Cooperation and Developments \(OECD\)](#) concepts to define AI and identify which of our systems uses AI.

We adopt the [Protective Security Directions](#) and [Protective Security Policy Advisories](#) issued by the Department of Home Affairs (HA) under the [Protective Security Policy Framework](#). This includes preventing staff from accessing AI productions, applications and web services that pose unacceptable risk to the Australian Government. We also apply DTA's [Agency guidance on public generative AI](#), which implements HA's [PSPF Policy Advisory 001-2025](#).

Additional resources

Here are some relevant resources to support your AI journey:

Learning and development

- [AI in government fundamentals course](#)
- [GovAI – Enabling AI Use Across the APS](#)

Internal Policy and principles

- Finance's [AI Transparency Statement](#)
- [Data Ethics Framework](#)
- [Acceptable Use Policy](#)
- [Privacy Policy](#) & [Privacy Act 1988](#)

External Policy and principles

- [Australia's AI Ethics Principles & Pilot Australian Government AI assurance framework](#)
- [Policy for the responsible use of AI in government](#)
- [Guidance on managing records created using AI](#)
- [Staff guidance on public generative AI & Protective Security Policy Framework](#)

Other Resources

- [AI for Finance Action Hub](#)
- [AI for Finance Intranet page](#)
- [Artificial Intelligence Feedback and Incident Register](#)