AI Policy

About this document

What this document covers

This document describes VAGO's approach to safe, responsible, and productive use of AI. It covers:

- our AI principles
- our risk appetite
- roles and responsibilities
- using public generative AI apps safely

Who this document applies to

This policy applies to:

- all VAGO employees
- any workplace participant including contractors, consultants and third-party service providers representing or acting on behalf of VAGO. This includes Audit Service Providers (ASPs) and other individuals or entities appointed to act on behalf of VAGO.

For convenience, they are collectively referred to as 'employees' in this policy

Risk appetite

VAGO supports the safe and responsible use of AI.

We have a moderate-risk appetite towards innovative practices but a low-risk appetite towards practices that contravene our AI principles.

Roles and responsibilities

Some staff have specific roles relating to AI.

Role	Responsibilities
Auditor-General	• Set the direction and be accountable for safe, lawful and ethical AI use
Deputy Auditor-General	• Approve the AI Policy and all high-risk AI use
Chief Information Officer	• Oversee AI governance and compliance with laws and standards • Approve and manage secure AI apps and technical controls • Proactively monitor AI use, oversee privacy impact assessments and incident response
Director - Data Analytics and Systems Assurance (DASA)	• Oversee the communication and deployment of AI tools across VAGO • Provide support for all staff to use AI tools • Help staff identify AI uses, additional training needs and other specialist assistance • Monitor usage patterns and training completion, and report adoption and issues
Executive leaders (directors and	• Set the tone for ethical, lawful and effective AI use within your division or team, ensuring AI use aligns with our AI principles and polices

business unit heads)	• Promote a digital mindset focused on efficiency and continuous improvement. • Support and guide the use of AI in engagements, ensuring it is applied effectively, ethically, and in accordance with audit quality standards.
Digital leaders - AI	• Experiment and pilot AI uses • Develop and organise training tailored to our needs and build this into existing learning and development curriculums • Collaborate with specialists (for example, DASA) to support our AI rollout
Engagement leaders	• Accountable for the overall quality of the engagement, including integration of AI.
Team leaders	• Operational lead for day-to-day engagements activities, ensuring effective application of AI within the engagement.
All staff	• Use only approved AI apps for all non-public information • Keep human oversight, verify outputs and maintain records

AI principles

Our AI principles

All staff must apply the following principles when using AI.

Principle	Description
Accountability	*We are accountable for our work and decisions*. **What this means: AI is not a substitute for human decision-making.** We exercise careful judgement and validate inputs and outputs when using AI. We are accountable for our decision-making.
Human rights	*We use AI to benefit individuals, society and the environment.* **What this means:** We use AI responsibly to improve our productivity, the quality of our work and the lives of Victorians. We avoid uses that reduce public trust. We protect stakeholders' rights and minimise potential harms.
Lawful, private and secure	*We use AI lawfully and protect information through privacy and security practices.* **What this means:** We use information in line with our privacy and security policies. We use approved AI tools for non-public information. We do not enter non-public information into public AI tools.
Transparency and contestability	*Our use of AI is transparent, documented and open to challenge.* **What this means:** We clearly communicate how we use AI. We monitor and review where and how we are using AI. We are open to discussion and challenge about our use of AI.
Fairness	*We identify and mitigate bias.* **What this means:** We understand, identify and address any bias in AI tools. We prevent discrimination and promote fairness and inclusivity.

Using public generative AI apps safely

What is a public GenAI app?

Any AI service on the public internet that accepts prompts and generates content outside VAGO's secure environment. Examples include ChatGPT, Grammarly, Google Gemini, Perplexity, Claude.

Using public GenAI apps

Only enter public information into public GenAI apps.

Only enter non-public information into approved enterprise apps provided by VAGO.

Essential rules

Do's and Don'ts

Do ...	Don't ...
use only approved enterprise apps for any non-public information. Document prompts and record any data entered into AI apps.	enter non-public, confidential, sensitive or personal information into public GenAI apps.
disable training settings and select privacy-protecting settings where available.	upload non-public datasets to public GenAI apps or paste client/audit evidence.
understand what the app you are using does, your objective, and how the app will help you achieve your objective,	forget requirements of Australian Auditing Standards, APES 110 and other requirements still apply.
treat outputs as unverified. Corroborate with authoritative sources before using outputs in official work.	allow AI to make or automate decisions for VAGO without human review and approval.
maintain human oversight and accountability. Add your reasoning and references to demonstrate how you made your decision.	use AI-generated content that infringes copyright, human or intellectual property rights.
disclose AI use in documents, reports or working papers.	use unapproved AI plugins, extensions or websites.
use multi-factor authentication and keep all accounts secure.	share your accounts details with anyone.
ask your manager, privacy officer or the IT team if you are unsure about how to use public GenAI apps.	use AI-generated code without approval from the CIO.
report suspected mistakes or breaches of these rules immediately via the Security Incident Management Procedure.	keep mistakes or breaches of these rules or other policies or procedures a secret.

Glossary and references

Glossary of terms

Term	Definition
Generative AI (GenAI)	AI that creates new content (text, images, code, etc.) based on prompts, for example, ChatGPT is a generative AI app.
Approved enterprise app	An AI app vetted and authorised by VAGO for internal use, with security and privacy controls in place.

High-risk AI use	AI use where the data involved, the decision they influence, or the control environment, could reasonably cause significant harm to individuals, VAGO, or public trust if they fail or are misused
Public AI app	Any AI service available on the open internet (for example, ChatGPT free version) that is not integrated into VAGO's secure environment.
Prompt	The text or question entered into an AI app to generate a response.
Public information	Information that is lawfully and freely available to the public (for example, published reports, media releases, legislation).
Non-public information	Information that is not publicly available, including client data, internal documents, financials, evidence or sensitive material (even if de-identified).
Sensitive information	Data that could cause harm if disclosed, including personal, financial or audit-related details.
Third parties	Organisations and individuals who are granted access to non-public information, including contracted Audit Service Providers (ASPs), consultants, and subject matter experts. All third parties must comply with the requirements set out in this policy.

References

Administrative Guideline for the safe and responsible use of Generative Artificial Intelligence in the Victorian Public Sector

Guidance for the safe and responsible use of generative artificial intelligence in the Victorian public sector

Information Security Policy

Charter of Human Rights and Responsibilities Act 2006

Privacy & Data Protection Act 2014 (Vic)

Public Records Act 1973 (Vic)

Protective Marking Procedure

Risk Management

Security Incident Management Procedure

Victorian Data Sharing Act 2017 (Vic)

Version control and reviewing frequency

Procedure review statement

This policy will be reviewed every 2 years from the last approval date, or when there is a significant change in the intent of this guidance.

Version release notice

Version	Date of effect	Amendment details	Amended by
1.0	12/09/2025	Initial release	CIO
Policy owner	Chief Information Officer		
Approved by:	Operational Management Group		Date: 17/09/2025