OFFICIAL

USE OF PUBLIC GENERATIVE ARTIFICIAL INTELLIGENCE PLATFORMS GUIDELINE

VERSION 1.1 EFFECTIVE OCTOBER 2024
CORPORATE MANAGEMENT GROUP

OFFICIAL

Australian National
Audit Office

Document control

Contact for enquiries and proposed changes:

Name	Chief Security Officer
Email	security@anao.gov.au
Location	Australian National Audit Office, 38 Sydney Ave, Forrest ACT 2603

Record of Endorsement

Status	Name	Position	Date
Approved	Danny Dawson	A/g Chief Security Officer	10 October 2024
Approved	Jacquie Walton	Chief Operating Officer	10 October 2024

Record of Amendments

Version	Author	Date	Review date	Comments
0.1	D Dawson	Aug 2023		Initial Draft
0.2	M Rigter	Jun 2024	June 2025	Updated to reflect revised DTA guidance from Nov 2023.
1.0	D Dawson	August 2024	October 2025	Updated to reflect ANAO clarity of guidance in the context of audit. Assessed guideline against the DTA Policy for the responsible use of AI government. Included references to DTA policy and guidelines where relevant.

Contents

1. Introduction

1.1 Accessibility of publicly available generative Artificial Intelligence (AI) platforms is rapidly evolving. The use of generative AI presents new and innovative opportunities, however due to the speed of evolution, the risks involved in their use need to be considered and assessed in the context of use at the Australian National Audit Office (ANAO).

1.2 The ANAO's guideline, *Use of Public Generative Artificial Intelligence Platforms Guideline,* outlines the conditions under which ANAO staff can use publicly available generative AI platforms, and where they cannot be used for official ANAO business.

1.3 This guideline applies to all publicly available generative AI platforms.

1.4 This guideline does not apply to enterprise generative AI platforms that ANAO may procure (for example Microsoft Co-Pilot) which will be governed by a separate guideline.

1.5 ANAO staff should only use publicly available generative AI platforms where there is no risk of information obtained in the course of performing an Auditor-General function and/or no sensitive information leaving the ANAO. In practice, this means no audit derived information can be used in publicly available generative AI.

2. ANAO Security Management Framework

2.1 The ANAO *Security Management Framework* outlines the ANAO's approach to protective security. The *Use of Public Generative Artificial Intelligence Platforms Guideline* document forms part of this framework.

2.2 This document is in line with the Digital Transformation Agency (DTA) Policy for the responsible use of AI in government[1]

2.3 This document also utilises requirements and recommendations contained in the Digital Transformation Agency (DTA) 'Interim guidance on government use of public generative AI tools'[2].

3. Document ownership and update

3.1 The Security Officer (CISO) is responsible for the periodic review and update of this document. The document will be reviewed for currency and applicability annually or sooner when required by changes in security risks or operating environment.

4. What is publicly available generative AI?

4.1 Generative AI platforms use information available on the internet to generate information outputs based on a user's inputs. User inputs can be questions or prompts that tools use to collate and generate responses back to the user. They typically use large language models (LLM) which are trained using data sets publicly available on the internet and by aggregating data inputted into the tools by users.

4.2 Publicly available generative AI platforms are third party platforms, tools or software that have not been security risk assessed by the ANAO nor has the ANAO entered into a commercial contract with a provider.

[1] Available at https://www.digital.gov.au/policy/ai/policy

[2] Available at https://architecture.digital.gov.au/guidance-generative-ai

4.3 Use of generative AI tools present risks for the ANAO, especially in relation to protecting the integrity and confidentiality of our information and the quality of the output used when using generative AI. Risks can cause significant reputational damage for the ANAO. Risks include:

- confidentiality breach of section 36 of the *Auditor-General Act 1997*;
- the generation of inaccurate, biased and/or factually incorrect data;
- privacy breach — unauthorised sharing of private personal information leading to fraud or other economic crimes;
- data breach — ANAO official, sensitive or classified information loaded into AI and subsequently used or accessed by other entities; and
- intellectual property infringement — AI may produce a result that infringes on existing copyright leading to legal and financial repercussions.

4.4 Use of publicly available platforms, such as ChatGPT and Bing AI, requires ANAO staff to be vigilant to the potential risks and benefits for each use case generative AI is being considered for.

4.5 This guideline has been written to assist staff when considering using publicly available generative AI tools. This includes ensuring staff understand what risks may apply, how to mitigate these risks and when these tools cannot be used.

4.6 The guideline aligns with the DTA's principles-based approach for the responsible use of AI in government.

5. Principles for use of generative AI

5.1 There are two core rules and four principles to follow to ensure the responsible, safe, and ethical use of publicly available generative AI by ANAO staff. They are designed to:

- support the responsible use of technology;
- reduce the risk of negative impact on those affected by AI applications;
- enable the highest ethical standards when using AI; and
- increase transparency and build community trust in the use of emerging technology by government.

5.2 Responsible and ethical use of publicly available generative AI is paramount. This is especially important in the context of the ANAO with the focus on the confidentiality of the information under the Auditor-General Act, integrity of data (and the data of audit entities) and the quality of audits - all critical to the Auditor-General's and the ANAO's reputation and accountability to Parliament.

5.3 Any use of these platforms must be consistent with the confidentiality obligations[3]in the *Auditor-General Act 1997* and related ANAO information security and data governance frameworks.

Core rules

5.4 When considering the use of generative AI tools, the potential benefits and risks for each use case must be assessed and appropriate steps must be put in place to mitigate these risks. If the risks cannot be mitigated to an acceptable level, the tools should not be used. Above all, apply these two core rules:

[3] https://www.legislation.gov.au/C2004A05248/latest/text

- You should be able to explain, justify and take ownership of your advice and decisions.
- Assume any information you input into public generative AI tools will become public. Do not input anything that could reveal classified, personal or otherwise sensitive information or information obtained in the course of performing an Auditor-General function.

Principle 1: AI should be used responsibly

5.5 ANAO staff should only use publicly available generative AI platforms where there is no risk of sensitive information or information obtained in the course of performing an Auditor-General function leaving the ANAO. In practice this means no audit derived information can be questioned in publicly available generative AI.

5.6 Use cases which currently pose an unacceptable risk to government and the ANAO include but are not limited to:

- information obtained in the course of performing an Auditor-General function;
- use of any non-public government data;
- use of official, classified, sensitive or confidential information;
- where services will be delivered, or decisions will be made; and
- where coding outputs will be used in government systems.

5.7 Any use of responses or outputs provided by these tools must be reviewed for appropriateness and accuracy, as they can provide incorrect answers in a confident way.

5.8 Consider whether the outputs meet community expectations, including in relation to the impacts of known biases in the tool's training data.

5.9 Consider intellectual property rights of third parties as well as broader privacy and copyright issues when using the tools.

Principle 2: Transparency and explainability

5.10 The information provided by public generative AI tools is often not verified, may not be factual, or may be unacceptably biased. Always question where this data comes from and be aware of the nature of the tool being used.

5.11 When using generative AI tools, you must be able to explain and justify your advice and decisions.

5.12 You should critically examine outputs from these tools to ensure those outputs reflect consideration of all relevant information and do not include irrelevant or inaccurate information.

5.13 You must ensure the ideas being generated are ethical and responsible.

5.14 You should make it clear when generative AI tools are being used to inform ANAO activities.

5.15 You should consider including markings in briefings and official communications indicating if AI was used to generate any of the information.

Principle 3: Privacy protection and security

5.16 Inputs into publicly available generative AI tools must not include or reveal classified information, personal information or sensitive information. This includes all audit information.

5.17 All activities need to align with legislation and policies relating to information and data. These include but are not limited to:

- *Auditor-General Act 1997;*
- *Privacy Act 1988*;
- Australian Government *Protective Security Policy Framework* (PSPF);
- *Information Security Manual*; and
- ANAO specific policies and standards relating to the security of information and assets.

5.18 Government and ANAO information must only be entered into these tools if it has already been made public.

5.19 You must not enter information that has been obtained through the course of performing an Auditor-General function. Any data stored in publicly accessible platforms is external to government and the ANAO and we do not know who has access to it.

Principle 4: Accountability and human centred decision making

5.20 Accountability is a core principle for activities within the ANAO. Generative AI tools must not be the final decision-maker on ANAO advice or services.

5.21 ANAO staff may consider using tools to brainstorm options or draft content in non-audit settings, however, content created must be reviewed by a human prior to use.

5.22 Always review the information generated by the AI tool to ensure the content aligns with your understanding of the issue and fact check the content using reputable sources.

6. Implementing the principles in practice

6.1 No audit derived information can be used in publicly available generative AI.

6.2 ANAO staff using publicly available generative AI platforms as part of ANAO work should use corporate credentials to sign up or log in.

6.3 Use your ANAO email as the user ID and create a new unique passphrase. Never use your ANAO user account password.

6.4 If a publicly available generative AI platform can be used without needing to create an account, do not create an account.

6.5 Where the option exists, turn off history and training options.

6.6 Do not distribute or click on any links provided or generated by public AI platforms or bots. These links could direct you to phishing sites or activate a malware download.

6.7 Only click on links from trusted sources.

6.8 Always treat with care any files generated by public AI platforms. They have the potential to contain malicious code, for example code disguised as a macro in Microsoft Office files. These files should always be considered as potentially malicious and not interacted with or distributed to other people until vetted and proven to be safe to use.

6.9 ANAO staff should report any instances where you are unable to fully apply this guidance to the ANAO Information Technology Security Advisor (ITSA) for further advice.

6.10 Immediately report any unexpected behaviour on your ANAO issued devices after using publicly available generative AI to security@anao.gov.au and to the ITSA.