Government of South Australia

# Guideline for the use of Generative Artificial Intelligence and Large Language Model Tools

DTF/G13.1

Across Government Guideline

## Purpose

This guideline explains the limitations and risks associated with the use of generative artificial intelligence (AI) and Large Language Model (LLM) tools within the South Australian (SA) Government. It provides SA Government agencies (agencies) with guidance on the safe usage of this technology and practical do's and don'ts in the interim while the long-term implications are considered.

## Scope

This guideline applies to all South Australian (SA) Government public sector agencies (as defined in ICT Policy Statement 1 – Compliant Authorities).

## Guideline detail

The rapid adoption of generative AI and LLM tools in our society, has highlighted the need to consider the safe use of such technologies within the SA Government context. The potential benefits of these tools need to be balanced against the limitations of the products and the risks of their use.

LLMs, a type of generative AI designed to generate text-based content, are first trained on associations within texts to create content similar to its training data. A key difference between traditional AI and generative AI is that the output of generative AI (including LLMs) is not designed to be 'accurate.' It is designed to be similar to content the model has 'seen' before, which can often be true to the original information or can be entirely different (and not factual).

## Benefits

Generative AI and LLM tools have the potential to automate a wide variety of tasks that may take a person days or weeks to perform, freeing up employees to focus on higher value work and to lift productivity.

The capabilities of these technologies can be applied to nearly all aspects of business. For instance, LLM tools can generate reports, create content marketing materials such as email campaigns and social media posts, create and debug code, create presentations, generate ideas, and help with brainstorming.

## Risk Management

While the potential of AI applications is extensive and growing, the technology is rapidly advancing and changing. Like every technology or tool, SA Government employees must remain responsible for their work and continue to meet all their obligations including those relating to record keeping, privacy, confidentiality, and integrity, ensuring the security of public sector data and responsible handling of personal information.

Prior to authorising the use of these tools, SA Government agencies should conduct their own risk assessments, balancing potential benefits and risk, while being aware that at this stage there are unknown and unknowable risks[1].

The adoption and use of generative AI and LLM tools may magnify existing information, cyber security and privacy risks and create new ones. SA Government agencies should assess the maturity of their existing security and privacy programs prior to implementation.

## Limitations and risks

There are several major limitations inherent with the use of generative AI and LLM tools, which must be considered and mitigated for acceptable SA Government use.

Refer to the table below for guideline details.

[1] Forrester: Build your own business case for Microsoft 365 Copilot.

| Limitations and Risks | Mitigating Controls |
|---|---|
| **General**<br>While generative AI and LLM tools are still evolving, comprehensive guidance is required to ensure appropriate use within agencies. | • Consider developing an agency strategy for the safe adoption of generative AI and LLM tools.<br>• Develop an agency policy governing the safe selection and use of generative AI and LLM tools that is regularly reviewed and updated, as required by the South Australian Cyber Security Framework (SACSF).<br>• Establish an AI governance and compliance framework for agency use.<br>  ○ Consider the National framework for the assurance of artificial intelligence in government and ISO/IEC 42001:2023 Information Technology-Artificial Intelligence-Management Standard.<br>• Properly identify and document the risks associated with the use of AI technologies.<br>• Conduct awareness campaigns for the safe and ethical use of AI tools.<br>• Define standard business use cases based on business needs and security risks. |
| **Information confidentiality**<br>Inputs into consumer oriented and open-source generative AI and LLM tools should automatically be considered as available in the public domain.<br>Employees can easily expose sensitive and proprietary government data in the questions and prompts they provide to generative AI and LLM tools. Any data provided into these tools is potentially stored | • Instruct employees via clearly understood and widely disseminated policies to not use prompts that expose official government or personal information. For example, such policies may include:<br>  ○ Disallow any cut-and-paste of enterprise content, such as emails, reports and chat logs into prompts.<br>  ○ Disallow any inputs that include customer data. |

| | |
|---|---|
| indefinitely, are likely stored outside of Australia, and may not be stored securely.<br><br>Data provided may be used to train third-party models in the future or used to generate responses to external users. Additionally, information provided to these technologies can potentially be viewed by service provider employees and subcontractors, future users of the system and hackers. | ○ Remind staff of their obligations under the Code of Ethics for the SA Public Sector and the SA Government Information Privacy Principles.<br>• Implement policies, staff awareness and technical controls to ensure that employees, contractors and suppliers do not use SA government information in AI products that have been assessed as posing an unacceptable level of security risk, such as DeepSeek.<br>• Consider a Data Loss Prevention (DLP) solution to monitor or control the egress information flows which contain sensitive information. Establish a self-hosted AI tenancy that is segregated from public networks and users (refer to Commercial Generative AI and LLM Services below). |
| **Data integrity and accuracy**<br><br>LLM AI tools are trained using immense data sets of internet-sourced data, including text scraped from unverified sources such as X, Wikipedia and Reddit.<br><br>Subpar training data can lead to responses that are insufficient, obsolete or contain sensitive information and biases, leading to biased, prohibited, or incorrect responses.<br><br>One of the most widespread and hard to spot problems in the AI context are 'hallucinations' where AI generates false information based on patterns and training data and presents it as fact.<br><br>It has been shown that AI not only hallucinates but also can amplify hallucinations.<br><br>Generally, manufacturers of consumer oriented and open-source AI tools ensure that their terms of use make no warranties as to the | • Enforce by policy a manual review model to spot incorrect or misinformed results.<br>• Manually review all model output and use it only as a first draft tool. Inaccurate or biased outputs could lead to liability, reputation loss or harm.<br>• Use in a controlled setting where generated text can be properly evaluated and tuned.<br>• Implement standard processes for configuration and change control among business operations and systems.<br>• If used for developing or checking code, ensure that secure software development principles are adhered to.<br>• Remain responsible and accountable for your work, including to critically assess all AI generated outputs and validate quality and accuracy with other sources. |

| | |
|---|---|
| accuracy or quality of the outputs, and the data it draws upon may not be current.<br><br>Agencies must remain accountable for the accuracy of all sources, including AI generated outputs, and should research and verify sources as required before they are used in their work.<br><br>Agencies should also ensure that any attribution obligations are met, with some AI tool manufacturers requiring users attribute the role it has played in drafting or editing content. | • Thoroughly understand terms of use and seek legal advice as necessary.<br>• Consider fine tuning models using specific internal data sources.<br>• Consider and monitor non-government suppliers use of AI when used in the provision of services of government. Seek assurance on their generative AI and LLM output validation processes. |
| **Legal and privacy**<br><br>Copyright<br><br>Users should be aware of the potential copyright violations with the use of generative AI and LLM tools. Terms of use usually put the responsibility to identify potential copyright violations in the output on the user. In some instances, manufacturers have also been accused of using copyrighted data for training models.<br><br>Legal Risks<br><br>Given the new and evolving nature of the AI technology, agencies should be mindful of broader legal risks, including in relation to any terms of use that apply. For example, it is usual for the terms of use to require users to indemnify the manufacturer for all losses resulting from misuse.<br><br>Privacy<br><br>The privacy policies and terms of use of these technologies are unlikely to meet the requirements of the SA Government to sufficiently protect personal or government information. | • Seek legal advice and conduct a compliance analysis and document the applicable regulatory and contractual requirements.<br>• Review the privacy policy / terms of use issued by the AI service provider regularly.<br>• Conduct privacy impact analyses on the AI business use cases.<br>• Establish or update the agency's privacy policies to accommodate the use of AI tools to meet applicable obligations - including in relation to integrity, privacy, security, human rights, anti-discrimination, administrative and other laws.<br>• Remind staff of their obligations under the Code of Ethics for the SA Public Sector and the SA Government Information Privacy Principles.<br>• Consider commercial products that include intellectual property indemnification coverage to copyright claims relating to the output of AI-powered products (for example, Microsoft commercial Copilot services, Adobe's Firefly and Google's Vertex and Duet AI systems). |

| | |
|---|---|
| **Ethics and fairness**<br><br>Relying on vast amounts of algorithms and data carries the inherent risk of bias or discriminatory content in outputs, and the algorithms used to generate outputs are largely unknown to general users.<br><br>The risk is particularly high where outputs may inform government decision making that have the potential to harm or impact adversely on individuals, and in the case of some manufacturers, the terms of use note that use in government context carries a greater risk of potential harm. AI systems have the potential to be expressions of cultural and social frameworks, representing the socially dominant concepts and normative ideas of the system designers. This can lead to inbuilt and amplified biases that could be particularly damaging for Aboriginal and Torres Strait Islander peoples and minority groups.<br><br>Data used for AI technology development and training could be insufficient, obsolete or contain sensitive information and biases, leading to biased, prohibited, or incorrect responses. Given these AI tools can also adopt different personas through text, there is also a potential risk of fraud or misuse:<br><br>• Deepfakes - These outputs generated by AI could appear realistic but are fake content. SA Government employees must be vigilant to identify fake news, misinformation, impersonations, or efforts to manipulate public opinion.<br><br>• Fraud and abuse - Malicious actors may use AI chatbots for writing fake reviews, spamming, phishing, and social engineering. Researchers have found many ways in which some platforms can aid in the development of malware. | • Regularly monitor and review use of AI tools to ensure they are being used responsibly ethically, safely, and according to law and government policy. Establish an incident reporting channel and investigation procedure to identify and handle the misuse of AI tools.<br><br>• Comply with the South Australian Government Artificial Intelligence Ethics Policy. This requires that agencies align to the Australian AI Ethics Principles when implementing AI-enabled systems. Agencies must assess the relevance of each principle to their specific use case and document how ethical considerations have been addressed.<br><br>• Where applicable, consider the use of generative AI and LLM tools through the lens of specific cultures, Aboriginal and Torres Strait Islander peoples and minority groups. Be wary of inherent biases that may be inbuilt and develop strategies to counter them. Where generative AI and LLM tools are used in circumstances that may impact Aboriginal and Torres Strait Islander peoples, agencies must consider the risk of negative bias in that instance and consult with Aboriginal and Torres Strait Islander peoples. Be vigilant and report on the identified events that violate the ethics principles.<br><br>• Consider the potential exploitation and attacks of the use of AI tools from external and internal malicious actors. |

| | |
|---|---|
| **Commercial Generative AI and LLM Services**<br><br>To reduce the information confidentiality risk associated with the use of consumer oriented and publicly available open-sourced generative AI and LLM tools or 'bring your own AI' (BYOAI), agencies should consider commercial generative AI and LLM products or privately hosted open-source tools, particularly where there are strict requirements that data must remain inside the M365 tenant or geographic boundaries.<br><br>All the other limitations and risks listed in these guidelines apply equally to commercial generative AI and LLM AI Services.<br><br>**Use of commercial generative AI and LLM services with OFFICIAL information**<br><br>The Australian Government have assessed that government information classified OFFICIAL, including information created for business operations and services, can be used with Generative AI providers certified under the Hosting Certification Framework, as well as Anthropic and OpenAI[2]. The SA Government recommends that agencies consider these providers when evaluating AI services for use with OFFICIAL information, on condition they also:<br>• Conduct their own risk assessments and technology approval processes to assess suitability.<br>• Consider the advice in this guideline, and relevant SA Government AI and security policies and guidelines. | • Continually monitor the security practices of the commercial generative AI and LLM services.<br>• Create information classification policies for the commercial generative AI and LLM services.<br>• Consider the data sovereignty risks:<br>  ○ Create limited use cases for out of region access.<br>• Ensure the general, data integrity and accuracy, legal and privacy, and ethics and fairness risks outlined in this guideline are properly considered.<br>• Depending on the use case, consider commercial generative AI and LLM products that offer sufficient protection for government information based on risk:<br>  ○ Establish a self-hosted AI tenancy that is segregated from public networks and users.<br>  ○ Establish commercial generative AI and LLM services with enterprise security considerations as an alternative to consumer oriented generative AI and LLM services. Consider potential data leakage risks.<br>• Assess the maturity of the agency information security program prior to implementation. |

[2] Australian Government, Department of Home Affairs, Protective Security Policy Framework, Policy Advisory 001-2025 OFFICIAL Information Use with Generative Artificial Intelligence.

| | |
|---|---|
| **Service Availability**<br>Agencies should identify the availability requirements of their AI services based on defined use cases and assess the impact to business operations should the service become unavailable. | • Conduct business impact analysis (BIA) on the AI services and document in business continuity plans (BCPs).<br>• Standardise the procedures of using the generative AI and LLM tools and implement alternative methods and workaround for service interruptions.<br>• Where appropriate, use generative AI and LLM tools as one output to your work (i.e., to supplement and accelerate, not replace). |

## Dos and Don'ts

**SA Government staff must not input any Personal Information or any official government information that is not suitable for public consumption into consumer oriented and open-source AI tools[3].**

| DO | DON'T |
|---|---|
| Assume that inputs into online generative AI and LLM tools will automatically be considered as available in the public domain. | Enter any information (questions or prompts) that shouldn't be in the public domain, including any information that is confidential. |
| Consult with your legal team on the tool's Terms of Service before use, including consideration of who owns the output and that terms of use can change at any time. | Enter any personal information about any person.<br><br>Enter any health information about any person. |
| Remain responsible and accountable for your work, including critically assessing all AI generated outputs and validating quality and accuracy with other sources. | Enter inputs or use outputs in a way that may breach another person's intellectual property rights. |
| Thoroughly research and source reliable references for content where necessary. | Use these tools for any query that is complex or sensitive, or where local context and nuance is critical. |
| Meet all your existing employment obligations- including in relation to handling official information, privacy, security, human rights, anti-discrimination, administrative and other laws. | Ask these tools to answer a question you don't already know the answer to or cannot validate the answer to - you need the knowledge to decide whether it can be trusted or contains bias. |
| Where required, attribute content that has resulted from the use of these tools. | Use these tools to replace your own research, analysis and content development or embed them into your work in a way that means it cannot be done without them. |
| Regularly monitor and review uses of these tools to ensure they are being used responsibly ethically, safely, and according to law and government policy. | 'Copy and paste' sections of AI-generated content into your work without attribution. If you do copy and paste any AI generated content, consider your obligations in relation to attribution and intellectual property. |

[3] Contact your agency ICT Service Desk and IT Security Advisor (ITSA) for advice regarding the suitability of AI tools and utilities for your intended use.

## Aboriginal Impact Statement

The needs and interests of Aboriginal and Torres Strait Islander peoples have been considered in the development of this guideline. As this guideline presents general guidance only, where generative AI and LLM tools are used in circumstances that may impact Aboriginal and Torres Strait Islander peoples, agencies must assess and consider the risk of negative bias and consult with Aboriginal and Torres Strait Islander peoples.

## Related Documents

- Australia's AI Ethics Principles
- National framework for the assurance of artificial intelligence in government
- SA Government Information Privacy Principles
- Code of Ethics for the SA Public Sector
- South Australian Cyber Security Framework
- South Australian Protective Security Framework
- SACSF Ruling 4 – Use of DeepSeek in the South Australian Government
- PC 030 – Protective Security in the Government of South Australia
- Protective Security Policy Framework
- Protective Security Policy Framework – Policy Advisory 001-2025
- Deploying AI Systems Securely | Cyber.gov.au
- OFFICIAL Information Use with Generative Artificial Intelligence
- Artificial Intelligence | Department of Treasury and Finance

## Document Control

| | | | |
|---|---|---|---|
| Approved by | CIO Steering Committee | Version | 1.4 FINAL |
| Approved date | 17 February 2026 | Next review date | December 2026 |
| Original date of approval | 31 May 2023 | Compliance | Optional |
| Contact email | Office for Artificial Intelligence artificialintelligence@sa.gov.au<br>Office of the Chief Information Officer OfficeoftheCIO@sa.gov.au | | |