Generative Artificial Intelligence (AI) tools developed for internal Government use.

WA Public Sector Guidance

What is generative Artificial Intelligence (AI)[1]?

Generative AI models generate novel content such as text, images, audio and code in response to prompts.

A large language model (LLM) is a type of generative AI that specialises in the generation of human-like text.

Which applications is this guidance applicable to?

This guidance applies to generative AI tools developed (either from scratch or from existing commercial AI models) to be used internally by government employees, using government information and data.

For example, an LLM trained on data contained in a government department's content management system, used for locating, summarising and answering questions about documents.

Who is this guidance applicable to?

- » All WA Government organisations and employees operating on behalf of the agencies.
- » Non-government suppliers and personnel that access WA Government information and resources.

What are some of the possible risks associated with generative AI tools developed for internal Government use?

- » Data leakage - Without adequate controls, sensitive government information may inadvertently be included in generated content, presenting a risk of unauthorised employee access to information.
- » Overreliance on AI – AI should always be used alongside human intervention.
- » Scalability and infrastructure – Developing, monitoring and maintaining AI systems can be resource intensive.
- » Cybersecurity - Malicious actors might target AI systems to compromise data, steal sensitive information, or disrupt government operations.
- » Bias and inaccuracy - AI systems can produce inaccurate and biased content and usage should mitigate bias and safeguard stakeholders. Content generated by the models should be checked for accuracy.

When you are procuring or using an AI solution for the first time at your agency, or for a different purpose, you must undertake a self-assessment against the WA Government AI Assurance Framework.

---

1   The definitions of 'generative AI' and 'a large language model' (LLM) are based on the definitions in Bell, G., Burgess, J., Thomas, J., and Sadiq, S. (2023, March 24). Rapid Response Information Report: Generative AI - language models (LLMs) and multimodal foundation models (MFMs).

DOs and DON'Ts for the safe, responsible and ethical use of generative AI tools developed for internal Government use:

DO	Don't
Familiarise yourself with terms and conditions specific to the AI application.	'Copy and paste' sections of AI-generated content into your work. If you do copy and paste any AI generated content, consider what your obligations are in relation to attribution and intellectual property.
Regularly assess outputs for accuracy and manage and mitigate bias	Rely blindly on AI without human oversight.
Regularly monitor and review uses of these tools to ensure they are being used responsibly ethically, safely, and according to law and government policy including considerations of the WA Information Classification Policy.	Rush development and implementation.
Have a robust monitoring and review process in place.	Engage and implement third-party AI services that have not undergone adequate security and risk assessments.
Always comply with relevant legislation (including the forthcoming PRIS legislation) of relevant jurisdictions that may impact upon the collection storage and use of data and information.	
Provide guidance for Government personnel and users about the capabilities and limitations of AI tools	
Assess your use case against the WA Government AI Policy.	

Use Case Examples

Joan wants to develop a generative AI model that can assist with reporting by drawing on historical government documents and real-time data to create summaries and documents.

What are some of the factors Joan needs to consider?

Joan should consider whether this is an appropriate use case for AI. An AI tool may lack the contextual understanding necessary to generate meaningful report insights or mitigate bias. It may also misinterpret data and produce inaccurate and irrelevant information. Joan should also consider whether knowledge and human expertise will be lost. Employees who would normally develop the reports would not develop as much understanding of the subject matter.

This guidance will be reviewed as AI evolves, and as risks are better understood.
For further inquiries or questions, please contact ai-dgov@dpc.wa.gov.au