GOVERNMENT OF
WESTERN AUSTRALIA

Government Public Facing Artificial Intelligence (AI) Chatbots (Large Language Models)

WA Government Agency Guidance

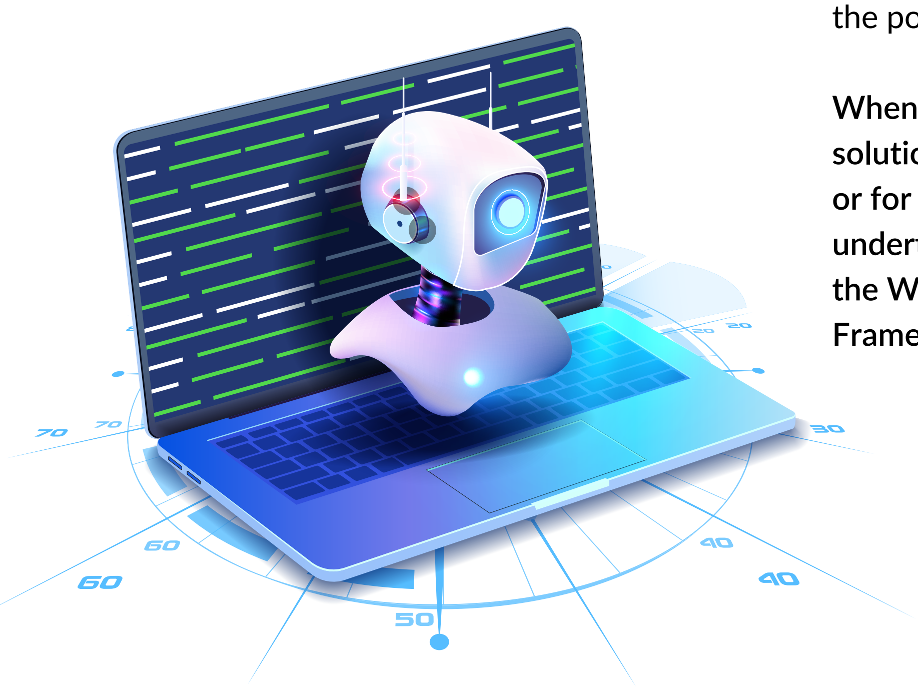
What are public facing chatbots/Large Language Models (LLM)?

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.

For the purposes of this document, Government public facing LLMs (chatbots) are applications which interact with the general public (users) through websites or applications to provide information/services in response to user-entered prompts. These are trained on and draw information from Government data.

An example of possible government application for a public facing chatbot is the use of an application embedded into a government website, which the public can 'chat' with to conduct detailed searches for information contained on the website.



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 public facing LLMs?

Some of the risks associated with LLMs relate to:

- ethics and fairness,
- legal and privacy,
- data integrity and accuracy and
- information confidentiality.

LLMs are trained on large amounts of data. Depending on the quality of this data, LLMs can produce inaccurate and biased or discriminatory results. Data provided (as prompts) may also be used to train models and generate responses to internal or external users, creating a risk of data leakage. Some of the main concerns associated with public facing LLMs are the risk of citizen data leaks, incorrect or inaccurate information being provided and the potential for bias in LLM outputs.

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.

DOs and DON'Ts for the safe, responsible and ethical development and deployment of public facing LLMs/chatbots

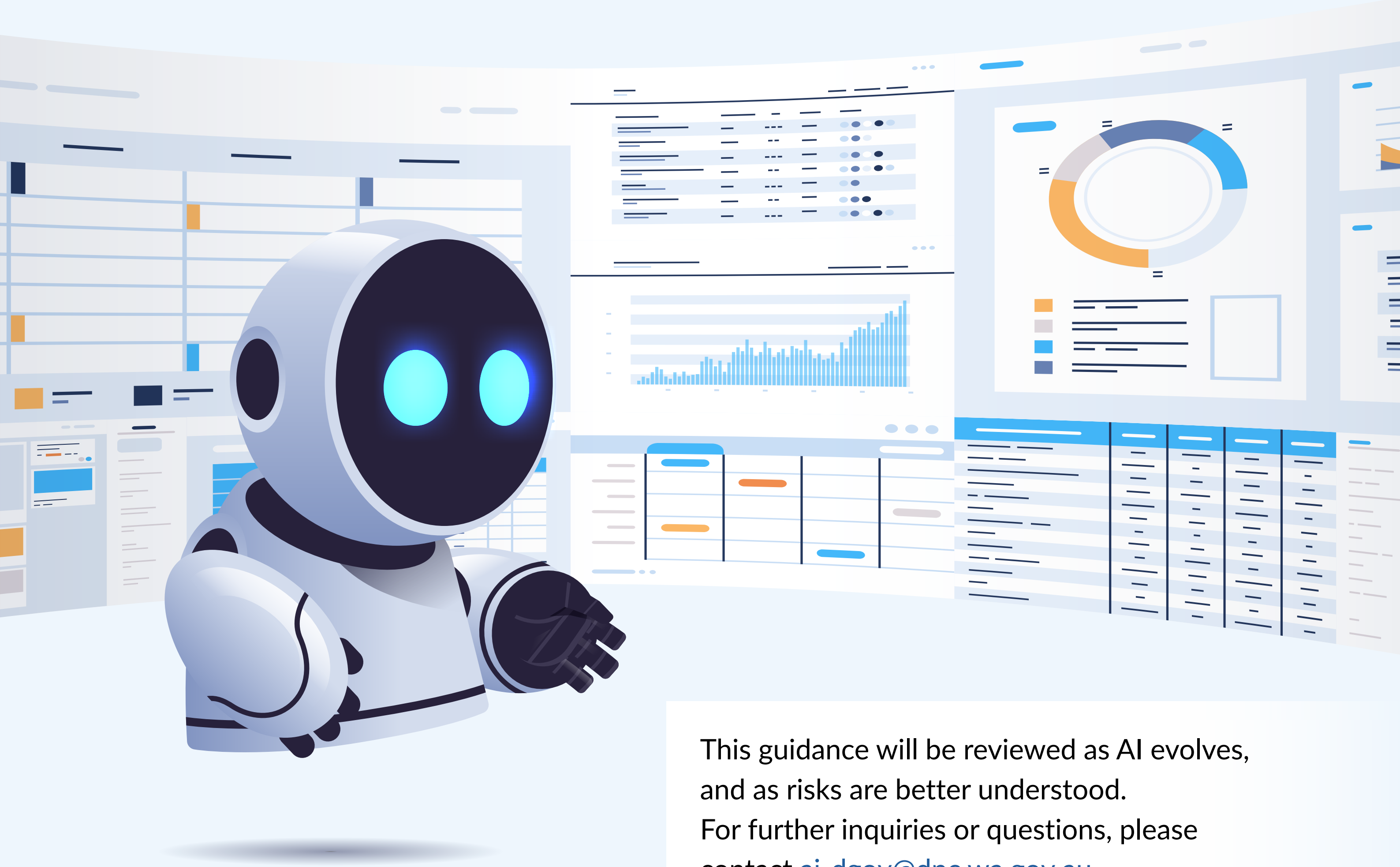
DO	Don't
Ensure clarity and transparency when users are dealing with a chatbot.	Implement AI as a complete replacement for human interaction. Some users would prefer human assistance.
Ensure that the Chatbots are implemented with clear governance and accountability.	Engage and implement third-party AI chatbot services that have not undergone adequate security and risk assessments.
Review the data used to inform the LLM to ensure it is accurate and any biases are mitigated.	Overcomplicate the chatbot's functions
Design chatbots with end-user design principles and make reasonable accommodations to ensure that all communities can access and use these services equitably.	
Develop these tools incorporating privacy by design principles and in adherence with applicable legislation (e.g. the forthcoming Privacy and Responsible Information Sharing legislation)	
Obtain consent for any data collection if applicable and include information statement clarifying what the data will be used for (if being used to inform AI).	
Conduct regular reviews and monitoring	
Make chatbot outputs as transparent as possible	
Clearly define the LLM capabilities and limitations	
Ensure that processes are designed to give public the opportunity to opt-out of engaging with AI systems and provide public with alternate pathways to conduct processes or interact with agencies to fulfill the service they require.	
Provide options for the public to escalate queries for human intervention and oversight.	

Use Case Example

Luis works for a public health department tasked with disseminating critical information about a new infectious disease outbreak. The department is overwhelmed with enquiries from concerned citizens, and the existing resources are struggling to keep up with the demand for information. Luis wants to develop and deploy a chatbot to help to answer simple queries from the public.

What should Luis do?

This use case poses a high level of risk, especially in relation to the information entered in the chatbot by the public, and the information the chatbot provides. Luis should conduct a risk assessment and consult extensively (including with his Legal team) to determine whether a chatbot is the best solution for the task. If Luis proceeds with developing and deploying the chatbot, he will need to be extremely mindful of legal and ethical considerations, including requirements for information privacy when access may cross jurisdictions (ie national/international).



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