Using public generative artificial intelligence (AI) tools safely

What is a public generative AI tool?

Any tool that is available to the public, takes user input and uses generative AI to create output. While generative AI technologies present opportunities for increased productivity across the NSW Government, they also introduce ethical, privacy and security risks that should be considered and addressed prior to use.

Examples include:

- ChatGPT (OpenAI)
- Copilot X (Github)
- BingAI (Microsoft)
- Gemini (Google)
- DALL.E
- MidJourney

What should you do?

Do	Don't
Fact check and verify outputs before using for any official purpose.	Allow generative AI to make decisions for the NSW Government.
Ensure outputs reflect consideration of all relevant information.	Use outputs that infringe on copyright or violate intellectual property rights.
Comply with applicable legislative requirements and laws.	Disclose or input personal, official, sensitive, classified or health information.
Disable training and logging features. Disable chat history.	Open any AI-generated links or files.
Enable multifactor authentication where available.	Use unofficial generative AI websites, applications or plugins.
Reference any AI-generated content.	Use AI-generated code in government systems and/or input or validate code from any government systems.
Seek advice from your privacy or security team if unsure or where guidance can't be found.	Ingest any government datasets unless approved and declassified by the data owner and/or IT Security team.

Users should follow their entity's internal policies on public generative AI tools in the first instance. If there is any doubt, contact your IT Security team or Chief Information Security Officer.

For the full version of the Cyber Security NSW generative AI end-user guidance, please contact: **info@cyber.nsw.gov.au**

Cyber Security NSW

Published October 2023