

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)



BardAI (Google)



DALL.E



MidJourney

What should you do?

Do

Fact check and verify outputs before using for any official purpose.

Ensure outputs reflect consideration of all relevant information.

Comply with applicable legislative requirements and laws.

Disable training and logging features.
Disable chat history.

Enable multifactor authentication where available.

Reference any AI-generated content.

Seek advice from your privacy or security team if unsure or where guidance can't be found.

Don't

Allow generative AI to make decisions for the NSW Government.

Use outputs that infringe on copyright or violate intellectual property rights.

Disclose or input personal, official, sensitive, classified or health information.

Open any AI-generated links or files.

Use unofficial generative AI websites, applications or plugins.

Use AI-generated code in government systems and/or input or validate code from any government systems.

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