

# **Generative Artificial Intelligence - Use by NSW Ombudsman officers**

## Document information

<b>Document name:</b>	Generative Artificial Intelligence - Use by NSW Ombudsman officers	<b>Type of document:</b>	Policy
<b>Status:</b>	Final	<b>Version number:</b>	1
<b>Date originally created:</b>	August 2023	<b>File reference:</b>	ADM/2023/234
<b>Superseded policy:</b>	N/A	<b>Compliance:</b>	All staff
<b>Related policies/ documents:</b>	<ul style="list-style-type: none"> <li>Code of Ethics and Conduct</li> <li>Cyber security policy</li> <li>Privacy and information management framework</li> </ul>	<b>Publication date:</b>	August 2023
<b>Review date:</b>	Annually	<b>Policy owner:</b>	Chief Operating Officer
<b>Distribution:</b>	Public	<b>Feedback:</b>	Legal, Governance and Risk Branch

### NSW Ombudsman

Level 24, 580 George Street  
Sydney NSW 2000

**Phone:** (02) 9286 1000

**Toll free (outside Sydney Metro Area):** 1800 451 524

**Website:** [ombo.nsw.gov.au](http://ombo.nsw.gov.au)

**Email:** [info@ombo.nsw.gov.au](mailto:info@ombo.nsw.gov.au)

© State of New South Wales

# Contents

## Contents

<b>1. Purpose</b> .....	<b>4</b>
<b>2. Application</b> .....	<b>4</b>
<b>3. Related legislation and policies</b> .....	<b>4</b>
<b>4. Key principles</b> .....	<b>4</b>
<b>5. Terms and concepts</b> .....	<b>5</b>
<b>6. Use of closed-access generative AI tools</b> .....	<b>6</b>
<b>7. Use of open-access generative AI tools</b> .....	<b>6</b>
7.1 Key risks .....	6
7.2 Prohibited uses of open-access generative AI tools.....	7
7.3 Pre-authorised uses of open-access generative AI tools.....	7
7.4 Protocols for open-access generative AI tools use.....	9
<b>8. Breaches of the policy</b> .....	<b>10</b>
<b>9. Roles and responsibilities</b> .....	<b>10</b>
9.1 Ombudsman.....	10
9.2 Executive .....	10
9.3 Officers.....	10
9.4 Manager Governance and Risk.....	11
<b>10. Ombudsman approval</b> .....	<b>11</b>
<b>Appendix A – Risk assessment template for other requested uses of generative AI</b> .....	<b>12</b>

## 1. Purpose

This policy governs when and how the NSW Ombudsman's Office (**Office**) may (or must not) use generative artificial intelligence technologies, including in the performance of Ombudsman statutory functions.

## 2. Application

The policy applies to:

- statutory officers appointed under the *Ombudsman Act 1974* (**Ombudsman Act**)
- ongoing, temporary and casual employees of the Office, and employees on secondment to the Office
- contractors and agency staff engaged to perform work for or on behalf of the Office
- students, interns and volunteers engaged with the Office for the purposes of work experience or in any other capacity, and
- consultants and others the Office has a business relationship with whose engagement requires adherence to this Policy.

In the policy, these people are referred to as '**officers**'.

## 3. Related legislation and policies

[Code of Ethics and Conduct](#)

[Cyber security policy](#)

[Privacy and information management framework](#)

The following documents have also been considered in the development of this policy.

- [NSW Government Artificial Intelligence Strategy](#)
- [NSW Government Artificial Intelligence \(AI\) Ethics Policy](#)
- [NSW Government Artificial Intelligence Assurance Framework](#)

## 4. Key principles

The evolution in artificial intelligence technology has resulted in increasingly sophisticated and accessible AI tools capable of significantly improving efficiency and service delivery. The Ombudsman recognises the potential for artificial intelligence technology to facilitate the performance of its statutory functions.

The use of artificial intelligence is not without challenges: how artificial intelligence tools are configured and operated can give rise to risks and consequences that undermine the work of the Ombudsman and harm the interests of its stakeholders.

The purpose of this policy is to provide direction and guidance to officers about the use of available AI tools. Its object is to ensure that this technology is available to the Ombudsman but in such a way that risks and consequences are appropriately managed and adverse consequences avoided.

Consistent with the *NSW Government Artificial Intelligence (AI) Ethics Policy*, the Office adopts the following overarching principles for the purpose of developing and implementing this policy:

- **community benefit** – AI should deliver the best outcome for the citizen, and key insights into decision-making. Use of AI should always be considered against other analysis and policy tools.
- **accountability** – Decision-making remains the responsibility of officers.
- **transparency** – The public/complainants will have access to an efficient and transparent review mechanism if there are questions about the use of data or AI-informed outcomes.
- **fairness** – Use of AI will include safeguards to manage data bias or data quality risks.
- **privacy and security** – AI will include the highest levels of assurance. Ombudsman and complainant data must be used safely and securely, and in a way that is consistent with privacy, data sharing and information access requirements.

## 5. Terms and concepts

**Artificial intelligence or AI** refers to computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. Many such systems are trained using **Machine Learning**, and have the capability to learn from or be trained by data it works with.

**Corporate function** refers to any function of the Ombudsman or an officer that applies by virtue of the Office's status as an entity however described (for example, a 'public sector agency', 'GSF separate agency' or 'auditable entity') and includes the employment and other corporate functions of the Office.

**Generative AI** refers to AI algorithms that can create (generate) new content in the form of text, images, audio or multimedia based on natural language prompts provided by humans. Generative AI may be:

- **Open-access generative AI tools**, which is any generative AI tool hosted on the internet that the public can use freely or by paid subscription. Some current examples of publicly available generative AI tools are ChatGPT and Google Bard. For the purpose of this policy, the definition of open-access generative AI tool does not include search engines or other similar sites that may use generative AI functionality (such as predictive text and autocomplete suggestions).
- **Closed-access generative AI tools**, which refers to a generative AI tool procured for use by the Ombudsman and which is not available to members of the public, or a generative AI tool that does not send Ombudsman information outside our network to train generative AI tools external to the Ombudsman. (As at the date of this policy, there are no **closed-access generative AI tools** in use.)

**Machine Learning** refers to a process involving a computer program that learns and adapts – either in a structured or unstructured way – by using algorithms and statistical models to analyse and draw inferences from patterns in data.

**Ombudsman statutory function** refers to any function conferred on the Ombudsman by the Ombudsman Act, *Community Services (Complaints, Reviews and Monitoring) Act 1993 (CS-CRAMA)* or any other legislation or legislative instrument that is not a corporate function, whether or not the function:

- is capable of being, or has been, delegated to any other officer, or

- has been delegated to, or directed or authorised to be undertaken by, any other officer in accordance with the Office’s Delegations and Authorisations Manual.

**Prompts** refer to the questions or instructions that an Officer enters into the Generative AI tool to generate a response.

**Risk assessment** refers to a risk assessment conducted using the methodology set out in the document at **Appendix A**.

## 6. Use of closed-access generative AI tools

Currently no closed-access generative AI tools are in use, or approved for use, by officers.

Any future use of closed-access generative AI tools will be subject to conditions determined by the Ombudsman at the time such a tool is developed and made available for use (and updated as and when required).

The conditions for use of closed-access generative AI tools will be based on a risk assessment. Refer to **Appendix A** for the risk assessment template.

## 7. Use of open-access generative AI tools

### 7.1 Key risks

The following table summarises some of the key risks of open-access generative AI, and how those risks are managed by this policy:

Risk	Policy - Mitigation/Control
Unauthorised disclosure of sensitive or other confidential information by its inclusion in a ‘prompt’ given to the generative AI tool	<p>Policy prohibits the inclusion of any sensitive or other confidential information in prompts (section 7.3).</p> <p>Policy prohibits certain uses that have a very high risk of inclusion of sensitive or other confidential information being included in prompts (such as decision making about complaints) (section 7.2).</p> <p>Policy requires approval for other uses that have a significant risk of inclusion of sensitive or other confidential information being included in prompts (such as editing or report writing) (section 7.4).</p>
Breach of Copyright, Breach of Moral rights to attribution and integrity of work, risk of plagiarism	<p>Policy prohibits the use of open-access generative AI to make decisions and perform work involved in writing public and other reports (section 7.2). Use of open-access generative AI for certain non-confidential content generation or content review is permissible (section 7.3) subject to restrictions and caveats.</p> <p>Policy requires all information be fact checked, which includes verifying sources and that the content is accurate (section 7.3).</p>
Incorrect, inaccurate or biased information, including ‘hallucination’	Policy requires ownership and accountability for quality content by fact-checking and citing AI generated content (section 7.3).
Malicious use and deception	Policy is to be read and complied with in conjunction with the Office’s Code of Ethics and Conduct.

Risk	Policy - Mitigation/Control
Lack of respect, care or compassion, and offence to the dignity of customers, if non-humans making decisions or communicating on matters personally affecting that customer	<p>Policy prohibits the use of open-access generative AI to make or assist in making substantive decisions, nor may it be used to assist in preparing written communication of decisions using confidential or sensitive information (section 7.2 and 7.3).</p> <p>Where open-access generative AI use has not been pre-authorized, Policy outlines considerations for individuals or communities, particularly for vulnerable members (Appendix A).</p>

## 7.2 Prohibited uses of open-access generative AI tools

Officers **must not** use open-access generative AI to perform, provide input into performing, or otherwise assist in performing, the functions of:

- (a) making any substantive decision in respect of any Ombudsman statutory function. This includes:
  - Decisions about the jurisdiction of the Ombudsman
  - Assessing complaints under the Ombudsman Act
  - Assessing complaints under CS-CRAMA
  - Decisions about what action to take in respect of a complaint (including whether to undertake preliminary inquiries, conciliation or investigation)
  - Assessing disclosures under the *Public Interest Disclosures Act 1994/2022*
  - Decisions about whether it is necessary or appropriate to refer a matter to another body
  - Decisions about the content of public and other reports, including how the factual findings and recommendations are expressed, and setting out what evidence is relied on.
- (b) forming any legal opinion.
- (c) communicating to a particular complainant about the handling of their particular complaint, for example in respect of the writing of an email or letter to a complainant about a decision made about their complaint<sup>1</sup>
- (d) other language translations or interpretations of communications and documents that are relied on in exercising statutory or corporate functions<sup>2</sup>
- (e) corporate functions such as data analytics or decision-making in recruitment activities, except where the data analysed or used for the decision is accessible to the general public (e.g. published statistical data, public NSW government policy and procedure documents).

Although officers are prohibited from using open-access generative AI tools for these functions, it may not preclude officers from using closed-access generative AI tools for these functions, subject to section 6.

## 7.3 Pre-authorized uses of open-access generative AI tools

Officers may use open-access generative AI to perform some types of tasks listed in this section without seeking Executive approval – **provided those tasks are not being used for the matters set out in section 7.2.**

<sup>1</sup> Note: However, open-access generative AI may be permitted to be used to assist in the development of a general template that might later be used during such particular communication with particular complainant.

<sup>2</sup> This includes website services such as Google Translate.

## Tasks

Assistance from open-access generative AI tools may only be used for tasks of the following general nature. (Approval is required for tasks not listed below):

- **Ideation** – brainstorming, generating or identifying counter-arguments
- **Writing** – copy-editing and proofing text, synthesising or summarising text from information that is not sensitive or confidential, generating social media content
- **Research** – identifying and summarising relevant publicly accessible literature, summarising and explaining complex concepts
- **Data Analytics** – identifying, analysing and projecting trends, and providing conclusions from publicly accessible data.
- **Information organisation** – summarising publicly accessible information, organising and formatting publicly accessible information, preparing chronologies from publicly accessible information
- **Presentation and training materials** – developing and synthesising training text and handouts, generating unique or specific content such as images, video and audio to match or enhance training materials, designing training and presentations materials

This list is subject to the restrictions and caveats below.

## Prompts

Officers must not include any confidential or sensitive information as prompts (or as part of a prompt) to an open-access generative AI tools. This includes:

- names or any other identifying information about any person (unless the information is public information about a public person relating to information in the public domain e.g. referring to a Minister’s public media statement, a judge’s published judgments or about a historic figure)
- any non-public [personal information](#) (within the meaning of the *Privacy and Personal Information Protection Act 1998*) about any person
- any [health information](#) (within the meaning of the *Health Records and Information Privacy Act 2002* about any person
- any information to which [section 17](#) (investigations to be conducted in absence of public) or [section 34\(1\)](#) (prohibition against disclosure of information) of the Ombudsman Act applies. If in doubt, advice should be sought from Legal ([legal@ombo.nsw.gov.au](mailto:legal@ombo.nsw.gov.au).)
- information that has or would have any of the following correctly applied classifications:
  - Sensitive (NSW Cabinet, Legal, NSW Ombudsman, Law Enforcement, Health Information, Personal, NSW Government).

## Ownership and accountability for product and quality

All AI generated content must be:

- **Critically evaluated.** Officers must assess whether the content includes any unfounded assumptions or biases. Furthermore, any ideas provided by the generative AI tool must be developed and edited such that they are substantially the officer’s own work.

Officers must exercise a high degree of care before relying on AI generated content that summarises technical or overly complex material (such as legislation, case law and standards).



- **Fact-checked.** Officers must ensure all information is accurate and up-to-date. This includes verifying and attributing to sources, checking statistics, and ensuring that any claims made in the content are supported by evidence. Any information relied upon that is obtained from a generative AI should be fact checked against a verifiable source.
- **Edited.** Officers must edit all content to ensure that it is sensible, well-written, structured in a logical manner and is appropriate for the intended audience. Any text taken from or based on text provided by the generative AI tool must be identified and rewritten so that it is substantially the officer's own work to avoid unwitting plagiarism / breach of copyright.
- **Proofed.** Officers must check all content for spelling and grammar, and consistency with Office style, before it is published or shared.

## Transparency

Officers must cite when open-access generative AI content has been used to assist with a task, whether in external or internal documents. An example citing reference is as follows:

\* A generative AI system was used to assist in copy editing and proof-reading parts of this document. No sensitive information was provided to the system, and the document has been reviewed and approved by the author for accuracy and appropriateness prior to signing.

## 7.4 Protocols for open-access generative AI tools use

### Check if intended use of open-access generative AI tool is pre-approved

Officers must check that any intended use of an open-access Generative AI tool is:

- not prohibited under section 7.2, and
- pre-authorised under section 7.3.

### Approved uses following risk assessment

If an intended use of an open-access Generative AI tool is prohibited by section 7.2 and/or not pre-authorised by section 7.3 of this Policy, approval may be sought and granted by the NSW Ombudsman or authorised delegate<sup>3</sup>) for that use following submission of a completed risk assessment. Refer to **Appendix A** for the risk assessment template.

### Training

Prior to using open-access generative AI tools, officers must undertake training on effective and safe usage in accordance with this policy from a pre-approved list of training. Completion of training will be recorded by the Manager Governance and Risk, who maintains a list of that training.

### Login

If open-source access generative AI is to be used for any office-related purposes in accordance with this Policy, officers must only use an account that has been created using their work email address. However, officers **must not** use the same password that is used to log into their Office account (e.g. their computer login).

<sup>3</sup> see Delegations and Authorisations Manual at 2021/115684.

Officers must not use any other open-source generative AI account (for example, an account created using their personal email address) for any office-related use.

### **Records management**

Officers must retain documentation each time generative AI is used, including screenshots of all prompts and outputs generated, and store the documentation in accordance with the Office's Records Management Policy.

Documentation related to authorised use of generative AI tools (including the appropriately completed risk assessment) should be sent to the Manager Governance and Risk who is responsible for registering authorised uses of generative AI.

## **8. Breaches of the policy**

Any non-compliance with this policy should be reported to managers in the first instance and copied to the Manager Governance and Risk.

Breaches will be evaluated by Manager Governance and Risk for further action under the Office's Privacy and Information Management Framework (e.g. reporting of any data breaches to the Information and Privacy Commission).

Breaches of this policy by officers may result in disciplinary action in accordance with the Office's Code of Ethics and Conduct.

## **9. Roles and responsibilities**

### **9.1 Ombudsman**

The NSW Ombudsman assumes ultimate ownership of this policy and either approves or delegates approval for exceptional circumstances that fall outside this policy.

### **9.2 Executive**

The Executive is responsible for the implementation of this policy in its entirety, including directing all officers in their teams, units, and branches to follow this policy.

### **9.3 Officers**

All officers are responsible for following the directives of this policy in its entirety.

Ombudsman employees managing external contractors and consultants with access to sensitive or confidential Ombudsman information should:

- ensure external contractors and consultants are made aware of this policy and its requirements and, if required, ensure that appropriate contractual provisions are included in procurement contracts to apply this policy to their work,
- check during the procurement stage whether generative AI tools are intended for use during the engagement and ensure any approvals required are obtained.

## 9.4 Manager Governance and Risk

The Manager Governance and Risk Officer is responsible for registering authorised uses of generative AI and compulsory officer training in accordance with this policy.

## 10. Ombudsman approval



Paul Miller  
**NSW Ombudsman**

## Appendix A – Risk assessment template for other requested uses of generative AI