Ombudsman
New South Wales

Use of Artificial Intelligence Policy

19 January 2026

Version 2

Document information

Document name:	Use of Artificial Intelligence Policy	**Type of document:**	Policy
Status:	Active	**Version number:**	2
Date originally created:	August 2023	**File reference:**	ADM/2023/234
Superseded policy:	Generative AI Policy, August 2023	**Compliance:**	All staff
Related policies/ documents:	• Code of Ethics and Conduct • Cyber security policy • Privacy and information management plan • Risk Management Policy	**Publication date:**	19 January 2026
Review date:	19 January 2027	**Policy owner:**	Senior Deputy Ombudsman, People, Performance & Sector Improvement
Distribution:	Public	**Feedback:**	Director, IT and AI

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
Email: info@ombo.nsw.gov.au

Contents

1. Purpose

The Ombudsman's Office (Office) recognises that, provided it is wisely designed and deployed, Artificial Intelligence (AI) has the potential - now and into the future - to support and improve our services and the public value and impact of our work. This may include by enhancing accessibility, improving customer experience, increasing the efficiency and effectiveness of information analysis and communication, and informing the better targeting of effort and resources.

This Policy implements the NSW Ombudsman's commitment to ensuring that any use of AI technologies by the Office is lawful, ethical and transparent, that risks are appropriately managed, and there is alignment with the Office's values, including Integrity Always.

This Policy applies in addition to, and does not replace or limit, existing obligations under the Office Code of Ethics and Conduct, or under any other applicable privacy, information access, cybersecurity, records management, or other policies.

2. Scope

2.1 Persons to whom Policy applies

The Policy applies to all persons engaged to do work for or on behalf of the Office, including:

- 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. This excludes any proprietary AI tools that contractors or agency staff may use while performing work for the office.
- students, interns and volunteers engaged with the Office for the purposes of work experience or in any other capacity.

This Policy also applies to any consultants and others the Office has a business relationship with whose terms of engagement require adherence to this Policy.

In this Policy, all of the above are referred to as 'officers'.

2.2 AI technologies and tools to which Policy applies

The Policy applies to any procurement, design, testing or use by officers of any AI technologies, including but not limited to:

- Traditional AI tools such as predictive models, classification systems or pattern detection algorithms
- Generative AI tools that create new content such as text, audio, images, or code in response to user prompts
- Agentic AI tools that use models, tools and data to identify tasks, and then take action autonomously to complete some or all of those tasks.

- Features and capabilities that are available or become available within a tool.

This means that the Policy applies to all of the following (referred to in this Policy as 'AI tools'):

- Open-access AI platforms hosted on the internet and available to the public, whether free or paid (such as ChatGPT, Gemini, Claude or similar tools)
- AI features embedded within Office-supported platforms or software (such as Microsoft 365 Copilot or Adobe Firefly)
- Office-supported or procured AI systems, including those hosted in secure environments and whether for internal use (such as Thompson Reuters Cocounsel) or for use by the public or stakeholders (such as the AI Assistant)
- Any research or trial use of AI tools by the Office, regardless of platform or function.

This Policy does not apply to:

- Standard spreadsheet formulas, basic auto-complete features and simple macros (eg Microsoft Outlook auto-forwarding rules)
- Traditional business intelligence dashboards and reporting tools (including Power BI)
- AI technology that may be embedded in general purpose applications (such as Google internet search, Google maps, social media) and that are not used with confidential or sensitive information.

If officers are in doubt as to whether this Policy applies to a particular tool or technology, they must consult with the Senior Deputy Ombudsman, People, Performance and Sector Improvement.

3. Overarching application of NSW Government AI Ethics Policy and AI Assurance Framework

The NSW Ombudsman is an independent statutory office, and the Office is a separate public sector agency. As such, it is not subject to the direction, control or policies of the NSW Government.[1]

However, the NSW Ombudsman has endorsed the NSW Government's Mandatory Ethical Principles for the use of AI for its own use, which therefore now apply as a policy of this Office.

The Mandatory Ethical Principles are set out in full in **Appendix A**, and provide that any AI must be:

- ***The most appropriate solution for a service delivery or policy problem***
- ***Used in such a way as to mitigate as much potential bias as possible***
- ***Used safely, securely, and in line with existing privacy and information access requirements***
- ***A solution that is open and transparent so that NSW citizens have access to efficient review mechanisms***

[1] Unless those policies are implement by legislation or legislative instrument that applies to the independent statutory offices, such as requirements imposed by way of a Treasurer's Direction under the *Government Sector Finance Act 2018*, provided the independent statutory office considers these to be consistent with the exercise of its statutory functions.

- ***A solution where the decisions are always subject to human review and intervention***

The NSW Ombudsman will also use the NSW Artificial Intelligence Assessment Framework (including as it may be amended from time to time) to assist with procurement, design and implementation of AI systems.

That includes a commitment to submit any proposal for the use of AI to the NSW AI Review Committee when required by the Framework, and in particular when any AI self-assessment conducted under the Framework in relation to a proposed use of AI identifies that the residual risk remains 'high' or greater following the application of all mitigation and controls.

4. AI Register

The office maintains a register (**AI Register**) of any AI tool that has been approved for procurement, design, testing or use (**registered AI tools**). The content requirements and form of the AI Register is in Appendix B.

Only the Ombudsman or the IT and AI Governance Committee may approve changes or additions to the AI Register, in accordance with this Policy.

The AI Register will be published (in accordance with section 7 of the *Government Information (Public Access) Act 2009* (GIPA Act)) on the Ombudsman's website, alongside this Policy. Particular information may be redacted only if there is an overriding public interest against disclosure under the GIPA Act.

5. Use of AI tools by officers

5.1 Prohibition on the use of unregistered AI tools

Officers may only use AI tools that have been approved and registered for use on the AI Register.

The use by any officer of any AI tool not on the AI Register (**unregistered AI tool**) is strictly prohibited. Approval (and registration on the AI Register) must occur before any steps are taken toward the procurement, design or testing of any AI tool.

5.2 Approved Use Cases of registered AI tools only

Officers may only use registered AI tools for an approved use case listed for that tool on the AI Register.

The use by any officer of an AI tool for any other use case is strictly prohibited.

5.3 Conditions of usage

Officers must comply with any conditions listed in respect of an AI tool and/or its approved use cases on the AI Register.

Appendix D sets out mandatory conditions that will be applied to all registered AI tools.

5.4 Ownership and accountability

Officers must verify the accuracy and appropriateness of all AI-generated outputs and take ownership and accountability for any material used or communicated. This includes:

- **Fact checking:**

  Officers must ensure all information is accurate and up to date. This includes verifying and attributing to sources, checking statistics, and ensuring that any conclusions made are reasonable and supported by evidence. Any information relied upon that is obtained from a generative AI should be fact checked against a verifiable source.

- **Critical evaluation:**

  Officers must assess whether the content includes any unfounded assumptions or biases. Furthermore, any ideas provided by an AI tool must be developed, reviewed and adopted so that it is 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).

  Officers must assess whether AI-generated content or analysis is based on incomplete, skewed or inappropriate data.

- **Editing:**

  Officers must review and edit all content to ensure that it makes sense, is well-written and structured in a logical manner, and is appropriate for the intended audience. Any text taken from or based on content generated by an AI tool must be identified and rewritten so that it is substantially the officer's own work.

- **Proofing:**

  Officers must check all content for spelling and grammar, and consistency with the Ombudsman's house style, before it is published or shared.

5.5 Records of AI generated content and AI Usage Log

Where an officer uses AI generated content to assist with a task, officers must make and retain comprehensive working documentation that clearly records that use, for example by keeping a record of the AI generated text and showing by mark-up how it has been edited.

Any internal Briefing Note or similar document that was, or includes any documents that were, prepared with the assistance of AI generated content, should include a statement that it includes AI generated content. (Example statement: *"[AI tool e.g. 'Co-Counsel'] was used to [outline use, e.g. 'assist with copy editing and proof-reading'] [document/s e.g. 'this Briefing Note']. Use was in accordance with conditions of the AI Register. All content has been reviewed and approved by the author for accuracy and appropriateness."*)

While a similar statement need not be included on externally published content, if any AI tool has been used to generate content or otherwise assist in the production of published or decision-related content (including reports, correspondence, presentations, media releases, social media posts) any such use must be clearly documented in the office's AI Usage Log (**Appendix C**).

5.6 Prohibition on any 'shadow' use of AI tools

Officers must not (for any office-related purpose) access or use, or cause any other person to access or use, any AI tool:

(a) on any personal/non-office issued laptop or device, or

(b) utilising any personal/non-office account, including any account established using a personal email login or other non-work issued credential.

This prohibition extends to the use of any AI tool, even if it is one that is on the AI Register and even if it is used for a permitted use case and otherwise in accordance with the conditions of the AI Tool and Use Case registration.

6. Procedure for approval of new AI tools or use cases

If an officer proposes an AI tool, or an AI Use Case, that is not currently authorised on the AI Register, they should speak with their branch Executive in the first instance. Following the approval from their branch Executive they may complete a briefing note outlining the tool, use case and including a completed NSW AI Assurance Framework self-assessment with the assistance of the secretariat of the IT and AI Governance Committee.

Further information on this process as well as the AI Tool and Use Case Register can be found on the AI Resources Intranet Page (AI Resources).

7. Incident management

Any adverse incidents involving AI must be reported to the Director, Strategy, Governance, Risk & Data, and managed in accordance with relevant policies, including Risk Management Framework and the Office's Privacy and Information Management Plan (e.g. reporting of any data breaches to the Information and Privacy Commission), including but not limited to:

- any unauthorised use of AI tools
- privacy breach
- the use of incorrect or unverifiable AI generated content
- biased content generated; or
- a lack of transparency in what inputs are used, or how content is created.

Before approving any AI tool for use, arrangements must be put in place to ensure that the office is able to promptly take any AI tool offline when necessary, including by maintaining documented manual processes as a fallback to ensure continuity of operations.

8. Duties and responsibilities

Role	Key responsibilities
Senior Deputy Ombudsman, People, Performance & Sector Improvement	• The designated senior leader who is the overall policy owner for AI, with the authority to govern its use across the organisation. • Champions, sponsors and maintains the organisation's AI policy and its commitment to lawful, ethical and transparent AI use. • Holds ultimate accountability for AI governance, including capabilities and risks. • Ensures adequate training is available to officers and those in AI related roles • Ensures that the AI Register is monitored for updates and changes to products on the register in both technology and handling of our data (e.g.: Privacy Policy changes from a vendor)
Director, Information Technology and AI	• The Director, Information Technology and AI is responsible for ensuring records of authorised AI Tools and Use Cases are kept as required. • Supporting the office in the training of users in the appropriate use of AI tools.
Director, Strategy, Governance, Risk and Data	• The Director Strategy, Governance, Risk and Data is the office's Chief Audit Executive and Chief Risk Officer and supports the IT and AI Branch with their AI risk and governance responsibilities.
IT and AI Governance Committee	The IT and AI Governance Committee will provide governance for all significant activity relating to adoption, configuration, usage and incidents relating to new and existing IT & AI solutions. This includes, but is not limited to: • AI Adoption, Oversight and Assurance • IT solution and service change and governance
Other Executives	• 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.
All Staff	All officers are responsible for complying with 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 AI tools are intended for use during the engagement and ensure any approvals required are obtained.

9. Breaches of the policy

Any non-compliance with this policy should be reported to managers in the first instance and copied to the Director, IT and AI.

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

10. Related legislation and policies

Legislation

- *Ombudsman Act 1974*
- *Government Sector Employment Act 2013* (including regulations and rules made under the Act)
- *Privacy and Personal Information Protection Act 1998* (including regulations, Codes of Practice and Directions made under the Act)
- *Health Records and Information Privacy Act 2002* (including regulations, Codes of Practice and Directions made under the Act)
- *Government Information (Public Access) Act 2009*

Policies

- Code of Ethics and Conduct
- Cyber security policy
- Privacy and information management plan
- Risk Management Policy

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 Assessment Framework

Guide to using AI Agents in NSW Government | Digital NSW

Guidance for AI Adoption | Department of Industry Science and Resources

11. Ombudsman approval

Paul Miller
NSW Ombudsman

Appendix A Mandatory Ethical Principles of the use of AI

Community benefit

AI should deliver the best outcome for the citizen, and key insights into decision-making

AI must be the most appropriate solution for a service delivery or policy problem. It should always be considered against other analysis and policy tools. AI should be the best solution that maximises the benefit for the customer and for government.

Projects should clearly demonstrate:

- that a clear community or government benefit or insight will be delivered
- that other solutions have been considered and ruled-out because they will not realise the benefits of an AI solution.
- that the use of the AI solution aligns with NSW Government priorities and/or the agency's strategic plans.

Fairness

Use of AI will include safeguards to manage data bias or data quality risks

The best use of AI will depend on data quality and relevant data. It will also rely on careful data management to ensure potential data biases are identified and appropriately managed. AI solutions that rely on sub-optimal quality data may result in sub-optimal project outcomes and recommendations. Algorithms that contain systemic and repeatable errors may lead to prejudiced decisions or outcomes.

Projects should clearly demonstrate:

- a data model that is designed with a focus on diversity and inclusion
- use of a dataset that is representative for the problem to be solved
- regular monitoring of data models and outputs.

Privacy and security

AI will include the highest levels of assurance

NSW citizens must have confidence that data used for AI projects is used safely and securely, and in a way that is consistent with privacy, data sharing and information access requirements. Any project outcome will be undermined by lack of public trust if there is any risk of a data breach or that personal data could be compromised.

Projects should clearly demonstrate:

- incorporation of privacy by design principles
- how information privacy, including potential for reidentification, and cyber security risks have been addressed
- agreement on the consent for data use, with sufficient information provided on how the data will be used to ensure informed consent

- that a rigorous assurance process against each of the five Ethical Policy Principles has been successfully completed.

Transparency

Review mechanisms will ensure citizens can question and challenge AI-based outcomes

Not only must the people of NSW have high levels of assurance that data is being used safely and in accordance with relevant legislation, but they must also have access to an efficient and transparent review mechanism if there are questions about the use of data or AI-informed outcomes. The development of AI solutions must be robust technically, legally and ethically. The community should be engaged on the objectives of AI projects and insights into data use and methodology should be made publicly available unless there is an overriding public interest in not doing so.

Projects should clearly demonstrate:

- a publicly available project objective and planned outcomes
- how the public can question and seek reviews of AI-based decisions
- how the community can get insights into data use and methodology
- how the community will be informed of changes to an AI solution, including where existing technology is adapted for another purpose.

Accountability

Decision-making remains the responsibility of organisations and individuals

AI is a powerful tool for analysing and looking for patterns in large quantities of data, undertaking high-volume routine process work, or making recommendations based on complex information. However, AI-based functions and decisions must always be subject to human review and intervention.

Projects should clearly demonstrate:

- that the agency remains responsible for all AI-informed decisions and will monitor them accordingly
- that human intervention in decision-making and accountability in service delivery are key factors
- that AI projects are overseen by individuals with the relevant expertise in the technology and its benefits and risks
- that a review and assurance process has been put in place for both the development of the AI solution and its outcomes.

Appendix B AI Tool and Use Case Register

The AI Tool and Use Case Register can be found on the AI Resources Intranet Page (AI Resources).

Appendix C AI Usage Log

The AI usage log can be found on the AI Resources Intranet Page (AI Resources).

Appendix D Mandatory conditions

The following conditions are to be applied to the use of all registered AI tools.

Condition	***Meaning***
1. Trained (Core AI) officers only	*Only officers who have completed the office's mandatory 'Core AI' training module may use an AI tool.* *It is a condition of use of AI tools that officers must have completed training on effective and safe usage from a pre-approved list of training. Completion of training will be recorded by the Learning & Development team, which maintains a list of that training.*
2. Officer to take ownership and accountability for use of AI generated content	*Officers must verify the accuracy and appropriateness of all AI-generated outputs, and take ownership and accountability for any material used or communicated. This includes:* ***Fact checking:*** *Officers must ensure all information is accurate and up to date. This includes verifying and attributing to sources, checking statistics, and ensuring that any conclusions made are reasonable and supported by evidence. Any information relied upon that is obtained from a generative AI should be fact checked against a verifiable source.* ***Critical evaluation:*** *Officers must assess whether the content includes any unfounded assumptions or biases. Furthermore, any ideas provided by an AI tool must be developed, reviewed and adopted so that it is 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).* *Officers must assess whether AI-generated content or analysis is based on incomplete, skewed or inappropriate data.* ***Editing:*** *Officers must review and edit all content to ensure that it makes sense, is well-written and structured in a logical manner, and is appropriate for the intended audience. Any text taken from or*

Condition	Meaning
	based on content generated by an AI tool must be identified and rewritten so that it is substantially the officer's own work. ***Proofing:*** *Officers must check all content for spelling and grammar, and consistency with the Ombudsman's house style, before it is published or shared.*
3. Explainability	*Officers must be able to explain how AI tools have been used, what role they played in shaping outputs, and what steps were taken to verify results.*
4. Recording AI use	*Where AI has been used to inform published or decision-related content(reports, media releases, public facing documents), this must be clearly documented in the offices AI Usage Log (Appendix C).*
5. Prohibited use cases:	
a. Recruitment decisions	*As directed by the PSC (Office of the Public Service Commissioner | Use of AI in Recruitment), "AI should not be used to filter out applications or make other decisions about candidates."*
b. Analysing government financial information	*As directed by Digital.NSW (Generative AI: basic guidance | Digital NSW), AI should not be used to analyse government financial information. AI "lacks the security and specialised expertise required to comprehend complex government accounting practices. Moreover, it carries the risk of introducing errors in budget allocation and financial analysis."*