

Artificial Intelligence Policy

1. Document control

Policy Number:	CD/26/8	Council Resolution Number:	2022-26/970
Document Owner:	Director Corporate Services, Strategy and Innovation	Document Author:	Manager Information Services and Technology
Approval Date	19 May 2026	Next Review Date:	19 May 2030

2. Statement of Intent

- 2.1. This policy establishes the principles for the ethical, transparent, responsible and secure use of Artificial Intelligence (AI), including Generative AI (GenAI), within The Barossa Council.
- 2.2. The Council supports the responsible use of AI to improve service delivery, support innovation, enhance accessibility, strengthen decision-making, and improve productivity where it can be used safely and appropriately.
- 2.3. AI must be used in a way that protects Council data, community information, privacy, confidentiality, public trust and organisational reputation. This policy is intended to enable safe use, not prevent useful innovation.

3. Policy Statement

- 3.1. AI can support Council work in many ways, including drafting, summarising, organising information, improving accessibility, generating options, supporting analysis, and helping staff work more efficiently.
- 3.2. AI outputs are not inherently accurate, complete, or authoritative. All AI-generated content must be reviewed by a human before it is relied upon, published, or used in decision-making.
- 3.3. Council acknowledges that AI can also support different working styles and accessibility needs, including helping some staff reduce cognitive load, structure information, and communicate more effectively.
- 3.4. AI must be used as a support tool, not a replacement for professional judgement, accountability, or critical thinking.
- 3.5. Staff remain responsible for the accuracy, legality, appropriateness, and final use of any work that includes AI assistance.
- 3.6. Where AI content is used, staff must verify important claims against reliable sources and, where relevant, identify the original source material.
- 3.7. Council will prefer AI use cases that deliver clear public value, improve efficiency, support inclusion, and align with organisational priorities and values.

4. AI types and use

- 4.1. AI includes, but is not limited to, GenAI, predictive AI, agentic AI, decision-support tools, automation tools and embedded AI features in software products.
- 4.2. AI may be used for low-risk tasks such as:
 - 4.2.1. Drafting internal text for review.
 - 4.2.2. Summarising public documents.
 - 4.2.3. Reformatting or plain-language rewriting.
 - 4.2.4. Brainstorming ideas.
 - 4.2.5. Supporting research using non-sensitive material.
 - 4.2.6. Assisting with accessibility and communication tasks.
- 4.3. AI must not be used as the sole basis for decisions that affect people's rights, services, entitlements or obligations unless the use case has been formally assessed and approved under Council governance processes.
- 4.4. AI can be used in higher value data analytics and decision making capacities when specifically applied to an opportunity in a secure and appropriate framework, including video and data analytics.

5. Data and confidentiality

- 5.1. Personal information, confidential information, commercially sensitive information, draft documents not approved for release, and other restricted Council information must not be entered into public AI tools.
- 5.2. Staff must treat confidentiality as time-sensitive. Information that is not yet public remains confidential until it is formally approved for release.
- 5.3. If there is any actual or suspected unauthorised disclosure of confidential or personal information through AI use, it must be reported immediately to the relevant manager and Information Services and Technology.
- 5.4. Where Council approves enterprise or closed AI environments, any data use must still comply with Council's privacy, security, records and legal obligations. Permission to use an enterprise tool does not create a blanket approval for all data types.

6. Considerations and Limitations

- 6.1. Misinformation and Bias
 - 6.1.1. AI may be trained in a way that leads to insufficient, incomplete or biased results, which, if relied upon, could lead to liability, reputation damage or other harm. The tool could, for example, overrepresent negative stereotypes, exclude a particular group of people or draw from data sets that are not relevant to Australian law.
- 6.2. Malicious use of data by third parties
 - 6.2.1. Cybercriminals may use AI chatbots for writing fake reviews, spamming, phishing, and social engineering. Moreover, researchers have found many ways in which some platforms can aid in the development of malware.
- 6.3. Copyright, trademarks and plagiarism

- 6.3.1. AI terms of use usually put the responsibility to identify potential copyright violations in the output on the user. Be aware that AI outputs may infringe copyright or intellectual property laws.
- 6.4. Hallucinations
 - 6.4.1. AI will meet all requests based on the structure of a user's instructions wording. If no data exists to meet the user's instruction the technology may create information. For instance, if you ask AI to provide the top 10 restaurants in an area and there are only 5 in that area, it may still return 10 answers, meaning 5 do not exist and are hallucinations. Officers must always check sources, seek to structure instructions to minimise the likelihood of hallucinations and also ask AI if you are unsure of its sources of information so you can cross check the data source.
- 6.5. Legal considerations
 - 6.5.1. At this stage, there is no legislation in Australia that specifically regulates the use of AI, the inputting of data into AI systems, and the use of information output from AI systems. However, AI results and outputs may be subject to other existing Australian laws, including privacy, consumer affairs, discrimination, copyright and intellectual property, defamation, and breach of confidential information, to name but a few.
 - 6.5.2. Officers must ensure that use of AI is consistent with their duties and obligations under legislation, any contracts to which the Council is a party and their own contracts of employment. Ultimately, any person who relies on a AI system is still accountable to the Council for their own work.
- 6.6. Considerations to reduce the risks of introducing AI tools within the Council include:
 - 6.6.1. Prioritise trial and implementation of secure AI technologies that offer protections from public access and utilise council owned data as its source.
 - 6.6.2. Prioritise AI applications that align with council objectives and values and have been approved under clause 7.1 of this Policy.
 - 6.6.3. Encourage innovation while safeguarding public interests and ethical standards.

7. Approved tools

- 7.1. Staff may only use AI tools that have been assessed and approved by Information Services and Technology and the Corporate Management Team.
- 7.2. AI tools that are assessed and approved must meet any standards established by either the Commonwealth, State or Local Governments, and an approved list will be maintained by the Manager, Information Services and Technology through our intranet.
- 7.3. Preference will be given to licensed, enterprise-grade tools that provide security controls, auditability, administrative oversight, and data protections suitable for Council use.
- 7.4. Public consumer AI tools may only be used where they have been explicitly approved for a defined use case and data classification level.
- 7.5. Unapproved AI tools must not be used for Council business.

8. Approval and trials

- 8.1. Any request to use a new AI tool or AI use case must be submitted to Information Services and Technology using the approved request process.

- 8.2. Requests should describe the purpose, proposed users, data classification, risks, benefits, controls, and whether the tool is public, enterprise, or embedded AI.
- 8.3. Short pilot trials may be approved for limited testing purposes where risk is low and safeguards are in place.
- 8.4. Trial periods should be time-limited and monitored, with a documented decision recorded before broader rollout.
- 8.5. Approval decisions should consider security, privacy, records management, legal compliance, accessibility, public value, and alignment with Council priorities.
- 8.6. Council may maintain a tiered approach to AI use:
 - 8.6.1. Prohibited: no use with sensitive, personal, or confidential information.
 - 8.6.2. Permitted with controls: enterprise or approved tools for internal, non-sensitive material.
 - 8.6.3. Encouraged: approved tools using public, published, or de-identified information.

9. Training and capability

- 9.1. Any staff member using AI for Council work must complete Council-approved induction or awareness training before use.
- 9.2. Training will cover responsible use, privacy, security, bias, copyright, verification, safe prompting, accessibility, and reporting concerns.
- 9.3. Council will provide refresher training and targeted guidance as tools, risks and business needs change.
- 9.4. Training should build capability, not merely compliance, and should include practical examples relevant to Council work.

10. Responsible use

- 10.1. Staff must ensure AI use is lawful, respectful, accurate and appropriate to the task.
- 10.2. Staff must check for bias, gaps, unsupported assumptions, hallucinations, and misleading outputs before using AI-generated material.
- 10.3. Staff must not use AI in a way that infringes copyright, misrepresents sources, breaches privacy, or produces offensive, discriminatory, defamatory or misleading content.
- 10.4. AI use must be transparent where required, and staff should be able to explain how AI contributed to a final product or recommendation.
- 10.5. Staff must keep appropriate records of material AI use where it affects decisions, advice, outputs, approvals or public-facing content.

11. Scope

- 11.1. This policy applies to all Elected Members, Employees and Volunteers within The Barossa Council.
- 11.2. This Policy is to be read in conjunction with other Council Information Services and Technology policies and processes.

12. Responsibilities

- 12.1. The Executive Leadership Team must:
 - 12.1.1. Ensure the ongoing provision of training on ethical AI use, data privacy, and security.
 - 12.1.2. Implement programs to raise awareness about AI technologies and their implications.
 - 12.1.3. Foster collaboration between departments to ensure consistency in AI policy application and sharing of knowledge.
 - 12.1.4. Develop a unified strategy for AI access across departments.
 - 12.1.5. Establish protocols for responding to incidents where AI systems fail or cause unintended consequences.
 - 12.1.6. implement mechanisms for reporting incidents and conducting investigations.
- 12.2. Employees must not:
 - 12.2.1. Deed sensitive corporate or personally identifiable information into an AI system.
 - 12.2.2. Rely on AI generated outputs without adhering to the principles of this policy.
- 12.3. Employees who are using AI systems must:
 - 12.3.1. Use AI to support human decision-making, not replace it entirely.
 - 12.3.2. Regularly assess and consider biases in AI systems to ensure implementation of AI in a manner that respects human rights, promotes fairness, and avoids discrimination.
 - 12.3.3. Mitigate any biases in AI systems to ensure fairness and equity.
 - 12.3.4. Prioritise transparency—AI processes and decisions must be explainable to the public and stakeholders.
 - 12.3.5. Implement data governance practices, including data anonymisation, data retention policies, data source transparency and consent management.

13. Legislation and References

- 13.1. This Policy is designed to ensure that the permitted use of Council's Information and Communications Technology (ICT) facilities is consistent with other relevant laws and policies regulating:
 - 13.1.1. Copyright, patent materials and other intellectual property
 - 13.1.2. Anti-discrimination
 - 13.1.3. Defamation
 - 13.1.4. Privacy
 - 13.1.5. Discriminator speech and the distribution of illicit and offensive materials
- 13.2. This following references also provide guidance on the responsible use of AI in Government:
 - 13.2.1. National Framework for the Assurance of AI in Government: Endorsed in 2024, this framework outlines transparency, administrative law, privacy, governance, accountability, and the monitoring and evaluation of AI systems in government usage. It includes practical tools and checklists for agencies designing and deploying AI.

[National framework for the assurance of artificial intelligence in government](#)

- 13.2.2. OAIC Privacy Requirements: The OAIC has released guidance on privacy and developing and training generative AI models.

[Guidance on privacy and developing and training generative AI models | OAIC](#)

- 13.2.3. Policy for the Responsible Use of AI in Government: Effective from September 2024, this mandates all Australian government entities (including local governments) to identify accountable officials and adhere to transparency, risk mitigation, and public statements relating to their use of AI. Agencies must also meet reporting requirements, such as publicly stating their AI use and ensuring accountability in decision-making processes.

[Policy for the responsible use of AI in government - Version 2.0 | digital.gov.au](#)

- 13.2.4. Australian Government Department of Industry Science and Resources: Australia's AI Ethics Principles and Voluntary AI Safety Standard (VAISS)

[Australia's AI Ethics Principles | Department of Industry Science and Resources](#)

- 13.2.5. Local Government Guidelines: South Australia's Local Government Information Technology South Australia (LGITSA) has published Generative AI Guidelines to help local councils address data protection and ethical considerations related to AI.

<https://www.lgitsa.com.au/wp-content/uploads/2024/11/LGITSA-Guidelines-Generative-AI.pdf>

14. Definitions

Generative Artificial Intelligence (GenAI)	Generative Artificial Intelligence - a range of technologies that leverage data, machine learning and prompts to create new data (such as text, images, video, audio and similar content)
Machine Learning (ML)	A subset of AI that involves algorithms and statistical models that enable computers to improve their performance on tasks through experience
Data Privacy	Protection of personal data from unauthorised access and ensuring individuals' control over their own data
Bias	Systematic and unfair discrimination in AI outcomes, often due to biased data or algorithms.
Transparency	The degree to which AI decision-making processes are open and understandable to stakeholders.
Generative AI	Generative Artificial Intelligence - a range of technologies that leverage data, machine learning and prompts to create new data (such as text, images, video, audio and similar content)
IS&T	Information Services and Technology Department
Hallucinations	Where Large Language Models may perceive patterns or objects that are non-existent, creating nonsensical or inaccurate outputs
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system
Personal Data	Information about a particular person, especially sensitive information relating to that person. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances, and

	may include information such as a person's name, signature, address (postal and/or email address), phone number, date of birth, photographs, IP addresses, voice print, biometrics and location information.
Phishing	An attempt by cybercriminals posing as legitimate institutions, usually via email, to obtain sensitive information from targeted individuals
Spamming	The sending of unsolicited, usually commercial messages (such as emails, text messages, or Internet postings) to a large number of recipients or posted in a large number of places
Deed	To "deed" information into a system means the formal, often legally binding, recording of data or documents into a digital repository or management system, typically transforming analogue (paper-based) information into a digital format.

15. Version History

This Policy will be reviewed by the Policy Author in consultation with the relevant stakeholders, within four years or more frequently if legislation or Council's need changes.

Version No.	Date.	Summary of Changes
1.0	19/05/2026	New Policy

16. Further Information

This Policy is available on Council's website at www.barossa.sa.gov.au. It can also be viewed electronically at Council's principal office at 43-51 Tanunda Road, Nuriootpa during ordinary business hours. A printed copy of this Policy can be obtained upon payment of a fixed fee.

Feedback regarding this Policy or its application can be made to the Customer Service Team on 8563 8444 or barossa@barossa.sa.gov.au in first instance, who will refer you to the most appropriate officer.