Strathbogie Shire Council

Generative Artificial Intelligence Policy

April 2026

Strathbogie SHIRE COUNCIL

Contents

Generative Artificial Intelligence Policy

Document ID:	SSCEDOC-43802981-505
Effective Date:	21 April 2026
Last Review:	New
Current Review:	April 2026
Date Adopted by Council:	21 April 2026
Next Scheduled Review Date:	April 2027
Responsible Officer:	Director People and Governance

PART 1 POLICY

1. PURPOSE

This policy provides guidance and procedures to govern the use of Artificial Intelligence (AI) by Strathbogie Shire Council (Council) at both an individual and organisational level.

The policy aims to ensure that AI technologies are used ethically, uphold legal standards and regulations, and benefit the community. Council supports the use of AI to enhance decision making, improve process efficiency and improve the efficacy of services within a secure framework considering privacy and the accuracy of information generated.

2. POLICY STATEMENT

The policy recognises the rapid evolution of AI technologies and their growing application across the public sector. It enables the appropriate, safe, and ethical use of generative AI within the organisation, while protecting data from unauthorised exposure.

Council fosters an innovation culture that encourages the responsible use of AI to augment human capability, enhance service delivery, drive efficiency, and respond to community needs in an environment where risks are appropriately identified, managed, and ethical standards upheld with clear documentation.

3. APPLICATION OF THIS POLICY

This policy applies to Councillors, employees, volunteers, contractors, and service providers who operate within Council's environment or handle information on behalf of Council.

Adherence to this policy is mandatory for all Council operations involving AI tools or technologies.

4. DEFINITIONS

Term	Meaning
Artificial Intelligence (AI)	Technologies that mimic human intelligence to perform tasks, learn from experience, and improve over time
Machine Learning (ML)	A subset of AI that involves algorithms and statistical models that enable computers to improve their performance on tasks through experience.
AI Tools	Software or platforms that use AI to assist with or automate tasks including content creation, analysis, or decision-making
Council	the Strathbogie Shire Council
Enterprise Generative AI Tool	A generative AI tool procured and managed by Council operating within a secure enterprise environment and integrated within Council's systems. Examples include tenanted Microsoft 365 Copilot, Chat GPT Enterprise, Duet AI for Google Workspace, Zoom IQ and Slack GPT
Generative AI	AI technology that creates new content or curates existing content, including text, images, music, code,

	and more, based on the data the technology accesses
Public Generative AI Tools	AI tools available to the general public that generate content based on user input. Examples include: ChatGPT, MidJourney, Bard, and Microsoft Co-Pilot (previously referred to as Bing Chat Enterprise)
Sensitive Information	Any data or information that could potentially cause harm, damage, embarrassment, or discrimination to an individual (or organisation) if it is disclosed, accessed, or used without authorisation
Confidential Information	Personal private information or proprietary information that is not in the public domain including business information e.g., Property Owner's Name, Rating information, Contract terms
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

5. ACCOUNTABILITY AND RESPONSIBILITIES

Role	Responsibilities
Councillors, employees, volunteers, contractors, and service providers	Are responsible for understanding and abiding by this policy and procedures at all times, and reporting privacy issues to the Coordinator Governance and Records Management
Director People and Governance	Responsible for this Policy and Procedure
Manager Digital Innovation and Technology	Responsible for updating this policy and providing technical input, implementing controls as directed by State and Federal Government agencies
Coordinator Governance and Records Management	Responsible for Information Management and Privacy

6. RELATED POLICIES AND LEGISLATION

The following Council, State, regional and national plans, and policies are relevant to this policy.

Legislation

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- *Victorian Charter of Human Rights and Responsibilities Act 2006*
- *Public Records Act 1973*

- *Freedom of Information Act 1982*
- Victorian Protective Data Security Standards
- Codes of Conduct for Victorian Public Sector Employees
- National Framework for the assurance of artificial intelligence in government

Related Council documents

- Privacy and Data Protection Policy
- Information Security Policy and Procedures
- Staff Code of Conduct CEO Directive
- Model Councillor Code of Conduct
- Health Records Policy
- Public Transparency Policy
- Records Management CEO Directive

7. GENDER EQUITY

We are committed to ensuring that all artificial intelligence systems are designed, developed, and deployed in ways that promote gender equality and prevent discrimination. Our approach recognizes that AI technologies can unintentionally reinforce existing biases, and we actively work to identify and mitigate these risks.

8. POLICY REVIEW

Council may review this policy at any time and at least twelve months from the date of adoption.

Minor amendments to the policy may be authorised by the CEO at any time where such changes do not alter the substance of the policy (eg a change to the name of a related document, or a change in legislation).

9. CHARTER OF HUMAN RIGHTS AND RESPONSIBILITIES ACT 2006 AND THE EQUAL OPPORTUNITY ACT 2010

The Council acknowledges the legal responsibility to comply with the *Charter of Human Rights and Responsibilities Act 2006* and the *Equal Opportunity Act 2010*.

The *Charter of Human Rights and Responsibilities Act 2006* is designed to protect the fundamental rights and freedoms of citizens. The Charter gives legal protection to 20 fundamental human rights under four key values that include freedom, respect, equality and dignity.

PART 2 PROCEDURES

AI Should Be Deployed Responsibly

Council employees, unless otherwise authorised, should only use AI platforms in low-risk situations and take the appropriate risk mitigation strategies described in this policy. Some examples of low-risk use include using tools to brainstorm ideas or options, or to do initial drafting of content, emails, and reports. Council must ensure that all uses of AI platforms comply with Council's Acceptable Computer Use Policy, Privacy Policy, and Records Management Policy.

AI functions which pose a considerable risk to Council include but are not limited to:

- Using any Council data considered to be sensitive or confidential.
- Services which will be directly delivered by AI, or decisions made solely by AI.
- Information or data which will be used in government systems. This includes IT code or information generated by AI.

The use of AI for any functions which may pose a considerable risk to Council should be considered by the ICT Team or approved by the CEO, prior to their application.

Note: Any outputs from AI must be reviewed by employees prior to it being input into Council systems or used to inform decision making.

Accountability and Human-Centred Decision Making

All users utilising AI must:

- Complete mandatory training prior to utilising AI systems
- Use AI to support human decision-making
- Use AI in a manner that respects human rights, promotes fairness, and avoids discrimination
- Regularly assess and consider biases in AI systems to ensure fairness and equity
- Regularly assess risk for each task where AI is employed
- Independently verify the validity of information provided by an AI system.

Users must not:

- Feed sensitive, confidential, or personally identifiable information into an AI system, unless the system is specifically approved for that purpose by the Information Management Team or CEO.

Users who are designing and implementing AI systems must:

- Implement AI in a manner that respects human rights, promotes fairness, and avoids discrimination
- Mitigate biases in AI systems to ensure fairness and equity
- Maintain comprehensive documentation of internally developed AI systems, including their purpose, functionality, data sources and decision-making processes
- Demonstrate appropriate risk assessment and establishment of controls
- Implement data governance practices, including data anonymisation, data retention policies, and consent management
- Ensure public facing AI systems are accessible to all, including people with disabilities, and consider the diverse needs of the community

- Include diverse perspectives and design principles in AI development and deployment processes.
- Implement systems for continuous monitoring of AI performance, accuracy, and impact
- Conduct periodic reviews and updates to adapt to new challenges and regulatory changes
- Follow established best practices for developing and testing AI systems, ensuring reliability, robustness and security
- Incorporate ethical considerations into the design and deployment phases
- Establish mechanisms for community and stakeholder feedback on AI deployments and use feedback to continuously improve AI systems and policies.

Procurement processes where AI systems are being considered ought to:

- Prioritise vendors committed to ethical AI practices and transparency
- Include ethical standards in the evaluation criteria for AI systems and vendors
- Establish protocols for evaluating third-party AI solutions to ensure they meet ethical and technical standards prior to onboarding
- Conduct risk assessments for each AI system being evaluated throughout the procurement process
- Implement contracts that contain stringent confidentiality, protection of privacy, data security, and intellectual property (IP) provisions to address AI-generated content not currently covered.

Senior Leadership must:

- Include AI as a standing agenda item in the IT Steering Committee
- Provide ongoing training on ethical AI use, data privacy and security including risks such as hallucinations and bias
- Implement programs to raise awareness about AI technologies and their implications
- Foster collaboration between departments to ensure consistency in AI policy application and share knowledge
- Develop a unified strategy for AI deployment across departments
- Establish protocols for responding to incidents where AI systems fail or cause unintended consequences
- Implement mechanisms for reporting incidents and conducting investigations.

The Manager Digital Innovation and Technology must:

- Oversee the ethical AI deployment, review policies, and address ethical dilemmas
- Conduct regular risk assessments to identify and mitigate ethical, social, and legal risks
- Remain abreast of new applicable developments in AI.

Council engages in a broad range of activities and delivers many services for the municipal community. Accountability is a one of Council's organisational values and as such those who use AI to produce content are responsible for that content and must be able to explain and justify their advice and decisions.

Any responses or outcomes provided by AI tools must be critically analysed for appropriateness and accuracy before being used, as they can provide incorrect or inappropriate answers in a confident way.

Council employees should consider:

- Whether responses or outcomes are factually accurate, meet community expectations, or influenced by known biases in the training data; and
- intellectual property rights of third parties as well as broader privacy and copyright issues when using these tools

Privacy Protection and Security

Any data entered into AI tools is likely to be stored externally to Council.

Inputs into AI tools should not include or reveal any classified information, including but not limited to commercial in confidence and proprietary documentation, or personal information held by council. All activities and inputs in relation to the use of information with AI tools should be considered a disclosure of that information and must comply with Council's Privacy and Data Protection Policy, relevant legislation, and the information privacy principles.

Generally, Council information should only be entered into these tools if it has already been made public or would be acceptable to be made public, unless the specific tool has been identified and approved for corporate use by the ICT Team or CEO.

Where possible de-identify information before entering it into an AI tool. For example, you want to use ChatGPT to draft a letter to a resident – enter a fictitious name and address into ChatGPT and then just modify the result it produces. Council staff must also not enter information that would allow AI platforms to extrapolate classified or sensitive information based on the aggregation of content you have entered over time. Additionally, Council must avoid sharing any information that could be used for identity theft, fraud, or hacking attempts. Where available, Council should disable any settings or permissions which save data or use history.

Compliance

- Ensure AI systems comply with local, state, and federal laws, including data protection and anti-discrimination laws on a regular basis
- Policy breaches must be escalated as per the Code of Conduct
- Breaches may result in disciplinary action.

Monitoring and Evaluation

Where a breach of this policy, whether accidental or intentional, is identified individual users and system and information owners are required to notify the Manager Digital Innovation and Technology immediately.

The Manager Digital Innovation and Technology will notify the Director People and Governance. Any breach of this policy will be handled within the Council policy framework, Code of Conduct and if appropriate, the Disciplinary Procedure.