



Artificial Intelligence Policy

Name of Council	District Council of Franklin Harbour
Responsibility	Risk Management
Revision Number	1.0
Effective date	September 2026
Last revised date	
Minutes reference	
Next review date	September 2028
Applicable Legislation	

1. Introduction

The District Council of Franklin Harbour ("Council") recognises the rising influence and use of Artificial Intelligence ("AI") in society and believes that the appropriate application of AI can increase efficiency and improve other aspects of operations within the organisation.

Generative Artificial Intelligence (GenAI) has become a highly accessible and rapidly growing technology that can offer many benefits to staff. There are various free and open-source technologies available wither as a standalone service (such as ChatGPT, CoPilot and Gemini) or embedded into other tools (such as Adobe Acrobat).

A key feature of GenAI is that its output is not designed to be accurate. It is designed to be similar to content the model has seen before, which can often be true to the original information or can be entirely different (and not factual).

GenAI is capable of performing the following tasks:

- Quickly sourcing, synthesizing, or summarising publicly available content;
- Creating or modifying images or videos;
- Rewording content in a particular style (for example, simple language, or language aimed at a particular reading age);
- Creating dynamic presentations;
- Generating ideas; and
- Generating alternative versions of work that you have created, to check whether you missed anything or could make improvements.

While these technologies may increase productivity, they create a range of risks that need to be proactively managed to protect organisational data, credibility and reputation.



Artificial Intelligence Policy

2. Purpose

This policy provides guidance to staff on the acceptable use of open-source and/or free GenAI at Council to ensure that AI is utilised in a secure and responsible manner and for specified uses, so that Council benefits from its use, while potential risks are mitigated and adverse consequences avoided.

3. Scope

This Policy applies to all employees of the Council, external consultants and contractors.

4. Definitions

Bias	An inclination or prejudice for or against one person or a group of people that is unfair.
Confidential Data	Data that the Council has determined as not being able to be share outside of the Council.
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)
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

5. GenAI is not a substitute for critical thinking

- 5.1 Staff are encouraged to experiment with GenAI tools to explore the potential benefits for their roles. However, GenAI tools are not a replacement for critical thinking or decision-making.
- 5.2 Staff cannot outsource their thinking to any technology. GenAI and other technologies can provide input to the decision-making process, but it cannot be relied upon to make decisions.
- 5.3 GenAI content may inform critical thinking and decision-making, but it is important to fact-check the content via other reliable sources.
- 5.4 Where content from GenAI tools is used, staff should consider where that content may have originated and the need to reference the originating source.



Artificial Intelligence Policy

6. Protecting personal or confidential data

- 6.1 No personal or confidential data is to be uploaded to GenAI products of any kind. To do so would effectively be publicly releasing that data.
- 6.2 Staff should always be aware that confidentiality can be a matter of timing. For example, a draft report that may become public is confidential until it is approved for release.
- 6.3 If staff become aware of a potential disclosure of confidential and/or personal data, it must be report to their manager immediately.

7. Limitations of GenAI

- 7.1 Staff who use GenAI technologies need to be aware of and mitigate the inherent risks and limitations of these technologies.
- 7.2 Specific limitations of GenAI include:

7.2.1 **Misinformation and Bias**

GenAI 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. GenAI can also suffer hallucinations. Always seek to verify the outputs of GenAI and do not ask it a question where the answer cannot be verified.

7.2.2 **Malicious use of data by third parties**

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.

7.2.3 **Copyright, trademarks and plagiarism**

GenAI terms of use usually put the responsibility to identify potential copyright violations in the output on the user. Be aware that GenAI outputs may infringe copyright or intellectual property laws.

8. Legal Considerations

- 8.1 At this stage, there is no legislation in Australia that specifically regulates the use of GenAI, the inputting of data into AI systems, and the use of information output from AI systems. However, GenAI activities 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 just a few.
- 8.2 Staff must ensure that use of GenAI is consistent with their duties and obligations under legislation. Ultimately, any person who relies on a GenAI system is still accountable to the District Council of Franklin Harbour for their own work.

9. Review and Evaluation

- 9.1 This policy will be reviewed to ensure that it remains up to date with the rapidly evolving technology and the legal framework that governs it.
- 9.2 Upon review the District Council of Franklin Harbour will communicate the updated Policy to all staff.



Artificial Intelligence Policy

10. Availability of Policy

This Policy will be made available on the Council's website, for inspection at Council offices and persons may obtain a copy of this Policy upon payment of a fee fixed by Council.

SIGNED:

Chief Executive Officer

Date: 17 / 9 / 20 26

Change History

Version	Issue Date	Change
1.0	September 2026	New Policy



Generative AI Guidelines

for Local Government in South Australia

Second edition, May 2026



Contents

Contents	2
Preface.....	3
1. Executive Summary.....	4
2. Background	6
3. Local Government Context.....	7
4. Opportunities of Generative AI	7
5. Legal Considerations	8
6. Recommended Actions	10
7. General Best Practice AI and Data Governance Advice.....	10
8. Guidelines and Resources	12
Appendix 1: Use Cases	13



Preface

LGITSA provides leadership and advocacy for the Local Government sector, with practitioner expertise across information, data and technology. Generative AI is now part of everyday work in councils, so we have refreshed this guidance to reflect the tools, laws and policies that apply in 2026.

These guidelines are a practical resource for all Council staff, Elected Members and stakeholders. They help you balance the opportunity and risk of generative AI, whether you use publicly available tools, enterprise tools embedded in your software, or AI features built into council systems.

This document is not a definitive strategy or policy. Use it as a starting point to inform discussion, provide quick reference education and consider how it could guide your organisation. It pairs with the LGITSA AI Adoption Toolkit, our sector-specific resource for South Australian councils.

The landscape keeps changing. This edition reflects the position as at May 2026, including the National AI Plan released in December 2025 and the updated Australian Government AI policy. As the sector matures we continue to update both this document and the LGITSA AI Adoption Toolkit.

Critical thinking and human oversight remain central to good governance and professional integrity. As tools become more capable they can still be confidently wrong, so the skill that matters most is informed human judgement: knowing when to use a tool, how to check its output and when to escalate to a person or an expert. This document is general information only and does not constitute professional or legal advice. Please consult your internal experts and service providers before you extend, embed, integrate or develop AI tools.

Feedback is welcome by email to info@lgitsa.com.au.



1. Executive Summary

Generative AI creates new content, such as text, images, audio, video and code, from a user prompt. It is now widely used through Large Language Model platforms including Microsoft Copilot, Claude (Anthropic), ChatGPT (OpenAI) and Google's Gemini. Many staff are becoming proficient in using these tools, which creates both opportunity and risk.

The key points throughout this document are:

- Approach generative AI as you would any other new technology. Understand the potential, the opportunities and the cautions for responsible use.
- You remain accountable for any output or AI-generated content you rely on or publish. No AI tool can outsource your thinking or remove your liability for a decision.
- Do not enter sensitive, personal or internal information into public generative AI tools. Assume anything you input could become public.
- Once you enter something into a public platform you have no control, guarantee, assurance or audit trail over how it is stored or used.
- Use the **LGITSA AI Adoption Toolkit** for sector-specific templates, governance support and worked examples tailored to South Australian councils.

Which AI tool can I use? Start with the data.

Public data	Internal data	Personal or sensitive data
Already public, or fine to publish on the council website. What you do A public tool is generally acceptable. Check the output and own the result.	Business or internal information not meant for public release. What you do Use a council-approved private or enterprise tool only. Anonymise first where you can.	Identifies a person, or is confidential or security classified. What you do Never enter it into a public tool. Approved systems only, with a lawful basis to use it.
Whatever the tool: you stay accountable, assume inputs could become public, and check every output.		

Guidance note: This document was drafted by LGITSA by a human author who added content, checked sources and verified the advice. AI tools assisted with drafting suggestions, all content was reviewed before publication.



2. Background

Generative AI refers to artificial intelligence (AI) that generates new outputs based on the data it was trained on. Earlier AI was typically designed to recognise patterns and make predictions on a controlled dataset. Generative AI instead creates new content from a user's prompts.

Since late 2022 we have seen a rapid pace of change, large investment, broad take-up and constant media attention. Capability has grown quickly. Tools now handle text, images, audio, video, live voice, multi-step workflows, autonomous agentic actions and increasingly act as assistants embedded in everyday software.

The policy landscape has matured since the first edition of these guidelines. Key developments relevant to South Australian councils include:

- **[National AI Plan \(December 2025\)](#)**. The Australian Government confirmed it will rely on existing technology-neutral laws and sector regulators, supported by voluntary guidance, rather than a standalone AI Act. The 2024 proposal for mandatory guardrails on high-risk AI was not legislated. A new Australian AI Safety Institute is being established in 2026.
- **[Policy for the responsible use of AI in government](#)**. First effective on 1 September 2024 and updated to version 2.0 on 15 December 2025. It applies to non-corporate Commonwealth entities, not councils, but sets a clear benchmark for accountability, transparency and governance that the sector can learn from. It is supported by an AI Impact Assessment Tool and guidance on AI procurement.
- **[Voluntary AI Safety Standard](#)** and **[Guidance for AI Adoption](#)**. The Department of Industry, Science and Resources published the Voluntary AI Safety Standard in September 2024, then released the Guidance for AI Adoption in October 2025. The Guidance superseded the Standard and is now the current national reference, setting out six essential practices for safe and responsible AI use by any organisation.
- **[Privacy Act reform](#)**. The Privacy and Other Legislation Amendment Act 2024 introduced new transparency requirements for automated decision-making. From 10 December 2026, entities must disclose in their privacy policy where a computer program uses personal information to make, or substantially help make, decisions that significantly affect a person. Councils should plan for this now.
- **OAIC AI guidance**. In October 2024 the Office of the Australian Information Commissioner published guidance on privacy and the use of [commercially available AI products](#), and on [developing and training generative AI models](#).
- **South Australian Government direction**. South Australia now has an [Office for AI](#), an [AI Ethics Policy](#) and a [guideline on the use of generative AI and Large Language Model tools](#). These apply to State Government agencies rather than councils, but contain valuable takeaways for the sector.

LGITSA has prepared this guideline with a South Australian Local Government lens. It is intended to be brief and to provide foundational awareness. As well as the links embedded above, further reading of the resources listed in Section 8 is recommended for all Local Government employees.



3. Local Government Context

The barrier to adoption is low. Many tools are free and available online and AI functionality is increasingly built into mainstream products. Microsoft Copilot is integrated across Microsoft 365 and AI assistants appear in browsers, search engines and line-of-business systems already on Council desktops. In many cases staff are using AI without realising it.

Some tools no longer just generate text. Known as agentic AI, they take actions on your behalf, such as sending messages, moving files or completing multi-step tasks across systems. Limit what these tools can access and require human approval before any action that affects records, people or money. They should not be given unattended access to internal Council systems.

Organisations must communicate the opportunities and risks clearly. Cyber security remains a top priority risk for Local Government. Technical controls matter, including email filtering, secure configuration, tested backups, endpoint detection, privileged access management and multifactor authentication. But the actions and awareness of the people using these tools remain one of the most important safeguards.

AI also lowers the bar for fraud. Convincing fake voices, video and text make impersonation, phishing and false invoice or supplier requests easier to produce and harder to spot. Verify unusual or urgent requests through a known channel and treat any request to change payment details with particular suspicion.

Everyone, including Elected Members, staff and volunteers, should be able to identify, assess and manage the risks of the tools they use. Constant pressure to do more with less means free and easy tools will keep drawing attention. The wish to save time while still producing quality work can lower a person's guard, and that is when mistakes happen.

Generative AI presents a real productivity opportunity. It is critical that the benefits and risks are made clear and that managing them is built into your procedures, training and development programs and cyber security strategy.

4. Opportunities of Generative AI

With balanced education, ethics and risk in mind, AI offers real opportunities. Given the right controls and human oversight, councils can use these tools to streamline processes and support better outcomes. Appendix 1 expands on the example ideas below, aimed at newer AI users. The LGITSA AI Adoption Toolkit provides comprehensive guidance and further sector-specific use cases.

Suggested use cases include:

- Creating a first draft of content.
- Summarising a public document or presentation.
- Exploring general information about demographics, markets and trends.
- Gathering ideas and different perspectives on a topic.
- Checking an Excel formula or the syntax of a code snippet.
- Drafting accessible or plain-language versions of public content.
- Evaluating an AI feature within a software product before adopting it.



5. Legal Considerations

Australia does not have a standalone law that specifically regulates generative AI. The National AI Plan, released on 2 December 2025, confirmed that existing technology-neutral laws and sector regulators will continue to apply, supported by voluntary guidance. This means inputting data into AI systems and using AI outputs may already engage existing law, including privacy, consumer protection, discrimination, copyright and other intellectual property.

One change to plan for is amendments to the Privacy Act. From 10 December 2026, new transparency requirements for automated decision-making take effect. Where a council uses a computer program that relies on personal information to make, or substantially help make, a decision that significantly affects a person, the council must explain this in its privacy policy. Councils should review where automation and AI touch decisions about residents and ratepayers and update their privacy policies before that date.

Employees must ensure their use of generative AI is consistent with their duties under the Local Government Act 1999 (SA) and other legislation, any contracts to which the council is a party and their own contracts of employment. Anyone who uses an AI system for output is still responsible for their own work and must be able to show how they reached a decision.

Entering data into a public generative AI system can cause a data breach. There is no guarantee that anything you input will remain private. Review contracts, agreements and terms carefully. For any non-public information, be clear about which systems are approved to receive, hold or process it.

There is an important difference between public and private (enterprise) AI environments, and all users should understand what the differences are. Treat a public AI platform like any public internet service that can access Council data. Understand what you put in, where it is kept, who can access it and who has rights to use it. Private (enterprise) AI systems can be treated like internal corporate applications, with the same need for contractual protection, business system assessments and information security classifications.

5.1 Cautions for data entered into public generative AI

Assume anything you enter could become public. Vendors may say inputs are not shared outside a session, but this may not hold in practice. Some consumer terms allow inputs and outputs to be used to improve the product. Free and consumer tiers often differ from paid or enterprise agreements, so know which terms apply to you.

All users should be aware that:

- You have no control, guarantee, assurance or audit trail once something is entered into a public generative AI platform.
- It is safest to assume that inputs into public generative AI tools could become available in the public domain.
- You should never enter personal, sensitive, confidential or security-classified information into a public tool.



5.2 Cautions for data output from any generative AI

Generative AI outputs may be wrong. Models can produce confident but inaccurate content, called 'hallucinations' and can reproduce bias from their training data. Capability has improved and many tools now cite sources or search the web, but outputs still need human review. Where an output describes a real, identifiable person, including inferred or fabricated detail, it may be personal information that must be handled under the Australian Privacy Principles.

All users should be aware that:

- You remain accountable for the forward use of any output or AI-generated content.
- You should be able to explain, justify and take ownership of your advice and decisions.

Australia's AI Ethics Principles, the Australian Government's guidance on using public generative AI tools and the Guidance for AI Adoption all reinforce these cautions and offer practical steps to reduce risk.

5.3 Intellectual property

Intellectual property remains contested for generative AI. Models are trained on very large datasets compiled from the internet, at times without clear permission. This raises questions about whether training infringes copyright and whether a user could face liability if a tool reproduces part of a copyrighted work without credit. Court cases in Australia and overseas continue to test these questions. Check originality before publishing AI-generated content and attribute the use of AI where appropriate.

5.4 Disclosing AI use

Be transparent about material AI use. Where AI has helped produce content that informs a council decision, a public communication or an official document, consider disclosing that use so readers can weigh it. The LGITSA AI Adoption Toolkit includes a Transparency Guide to help you decide when and how to disclose. This is separate from the automated decision-making transparency requirement described above, which is a legal obligation under the Privacy Act.

Guidance note: This section provides general information only and is not legal advice. Councils should seek their own legal advice on how these laws apply to their circumstances.

6. Recommended Actions

1. Use the LGITSA AI Adoption Toolkit to map your Council's maturity and refer to South Australian and Australian Government guidance for limitations, risks and controls.
2. Audit actual generative AI use across the organisation, including shadow use, and feed the findings into cyber security awareness, ethics and staff training.
3. Map where AI and automation touch decisions about residents and ratepayers, and update privacy policies before the automated decision-making transparency rules commence on 10 December 2026.



4. Review and update policies covering privacy, records, information technology, media and publishing to reflect generative AI use.
5. Scrutinise vendor and software contracts where AI is, or may be, embedded, and make sure they are clear on acceptable use for the entry and disclosure of Council data.
6. Review systems that hold sensitive or internal information, and publish information security classifications.

7. General Best Practice AI and Data Governance Advice

Start with the purpose

- Have a specific purpose linked to a business outcome and public benefit. Standard data governance still applies to AI and good governance matters more, not less.

Protect the data

- Consider the type of data you are working with. If it would go on the Council website, it is probably safe to use. If it is internal information, only a council-sanctioned (private or enterprise) tool should be used. Where any identifying detail is involved, it is best practice to anonymise or redact it first.
- Do not enter personal information about residents, staff or third parties into a public tool. You are responsible for that data and may have no lawful basis to disclose it.
- Consider privacy and ethics. Even with identifiers removed, AI can often re-infer sensitive attributes with high accuracy.
- Treat prompts and outputs as records. What you put into a tool and what it returns may be a public record and could be discoverable under freedom of information. Do not type anything you would not be comfortable putting in an email.

Protect your accounts and systems

- Do not reuse your work email and password to set up a consumer AI account. Where a personal account is needed, use a separate one with a unique password and ideally use your council's approved enterprise tools for work.
- Do not click on or share links generated by public AI tools without checking them. They may lead to phishing sites or malware. Only trust links from verified sources.

Get better, safer results

- Challenge outputs and ask for sources. These tools are built to sound fluent and helpful, which is not the same as accurate.
- Give context and a goal, not just a polished prompt. Telling the tool what you are trying to achieve and setting the scene without real names or sensitive detail often outperforms a perfectly worded one-off request. Specifics can be added back in after.
- Refine over several turns. Ask for more of one thing or less of another. The tool keeps the thread's context, so build on it rather than starting again. Newer agentic tools can also chain steps and use other systems, so be clear about scope and check each step.
- When in doubt, ask before you act. Raise unusual outputs, suspected data exposure or unfamiliar tools with IT or your manager early. Reporting a near miss beats cleaning up a breach.



8. Guidelines and Resources

LGITSA resources

[LGITSA AI Adoption Toolkit \(sector-specific guidance for South Australian councils\)](#)

South Australian Government

[Office for AI policies, standards and guidelines](#)

[South Australian Government AI Ethics Policy](#)

[South Australian Government guideline on use of generative AI and Large Language Model tools](#)

Australian Government

[National AI Plan \(December 2025\)](#)

[Policy for the responsible use of AI in government \(version 2.0\)](#)

[AI Plan for the Australian Public Service 2025](#)

[Guidance on using public generative AI tools](#)

[Guidance for AI Adoption \(current national reference, supersedes the Voluntary AI Safety Standard\)](#)

[Australia's AI Ethics Principles](#)

[OAIC privacy and the use of commercially available AI products](#)

Cyber Security

[ASD ACSC, Engaging with Artificial Intelligence](#)

[ASD Essential Eight](#)

[Opportunities for AI in cyber defence \(May 2026\)](#)

Other jurisdictions and standards

[NSW AI Assessment Framework](#)

[ISO/IEC 42001 AI management system standard](#)

[UNESCO Recommendation on the Ethics of Artificial Intelligence \(2021\)](#)

Legislation

[Local Government Act 1999 \(SA\)](#)

[Privacy Act 1988 \(Cth\)](#)



Appendix 1: Use Cases

These everyday examples show safe ways for newer users to get value from generative AI. For sector-specific and more advanced use cases, see the LGITSA AI Adoption Toolkit.

Use case	Safe approach
Creating a first draft of content	Ask for a structure, headings or a sample to get started, or to check your own draft for gaps. Do not enter council particulars. Review the output closely and own the result.
Summarising a document or presentation	Confirm the document is public and you have permission to share it, then use an approved tool to summarise or find key topics. Never upload sensitive, internal or confidential material to a public tool.
Exploring markets, trends or suppliers	Ask general questions about publicly available information. Never enter proposal or tender content. Treat outputs as possibly biased, inaccurate or fabricated, and verify against the source.
Finding an Excel formula or code syntax	Ask about a suitable formula or expression using a made-up example, not the real data. Even where a report is public, the underlying data often is not.
Gathering ideas and perspectives	Ask general questions about the area, community groups and interests, then check other sources for accuracy and local relevance. Use respectful language and assume your inputs may be visible elsewhere.
Creating an image for internal use	Use an approved image tool with general descriptions. Leave out internal particulars such as locations or access details. Check the image before use.

