

**ARTIFICIAL INTELLIGENCE – GENERAL POLICY**

F&amp;BS | 63/19/1-02 | #7890122

**RECOMMENDATION:****That Council adopts the Artificial Intelligence General Policy.****INTERESTED PARTIES:**

Not applicable

**EXECUTIVE SUMMARY:**

This report seeks Council's approval to adopt the Artificial Intelligence (AI) General Policy, which establishes a governance framework for the responsible, ethical and secure use of artificial intelligence technologies across Council operations.

The AI principles outlined in the policy are aligned with and informed by the Australian Government's National Framework for the Assurance of AI in Government (2024), Queensland Government regulatory frameworks and privacy legislation, while being tailored to reflect Council's business needs including our operational environment, governance requirements and community expectations.

Key safety features include strong human oversight, prohibitions on fully automated decision-making with substantial impact, safeguards against misuse and restrictions on non-approved tools. The policy also includes requirements relating to transparency, bias monitoring and accountability for AI-generated outputs.

The policy clearly establishes roles and responsibilities across Council, to ensure appropriate oversight, accountability and compliance with AI requirements and practices. This includes, responsibilities relating to governance, risk assessment, approval processes, monitoring, capability development and the responsible day-to-day use of AI technologies across Council operations.

This policy positions Council to leverage AI to improve operational efficiency, support informed decision-making and enhance service delivery, while ensuring appropriate governance, risk management and accountability.

**BACKGROUND:**

In response to the increasing role of AI across the public sector, including local government, Council has developed its first Artificial Intelligence General Policy.

Strategic oversight and rigorous due diligence have been applied to assess the implications of AI. This measured approach has enabled Council to move beyond market hype and develop an AI Strategy, together with the adaptation and further development of foundational AI Guiding Principles, providing a structured framework for the responsible, secure, and effective adoption of AI.

This technology presents opportunities to improve efficiency, enhance service delivery and support informed decision-making. However, the use of AI technologies introduces potential risks, including data privacy concerns, potential bias, inaccurate or misleading information and cybersecurity considerations. In recognition of these opportunities and risks, the development of a formal policy is considered necessary to guide the responsible application and use of AI technologies across Council.

#### **COMMENT:**

The proposed policy outlines a set of clear principles and requirements to ensure AI technologies are used in a responsible and controlled manner across Council.

Key focus areas include:

- ***Transparency and Ethics:*** The technology is used ethically and transparently, ensuring AI-generated outputs and decision-making processes can be appropriately understood, explained and disclosed, where required.
- ***Human Oversight:*** The policy mandates a human-in-the-loop approach, ensuring AI systems support rather than replace human judgement, expertise and accountability.
- ***Accountability:*** The policy establishes clear governance arrangements, roles and responsibilities to ensure appropriate oversight, approval, monitoring and responsible use of AI technologies.
- ***Data Protection:*** Outlines requirements relating to privacy, cybersecurity and information management, including limitations on the use of public generative AI tools and the protection of confidential and sensitive information.
- ***Ongoing Monitoring:*** Requiring AI systems, practices and associated governance controls to be regularly reviewed and updated to reflect technological advancements, legislative changes and evolving community expectations.

The policy supports a balanced approach, enabling Council to leverage emerging technologies while maintaining community trust and strong governance practices.

#### **OPTIONS:**

##### **Option 1 (Recommended):**

That Council adopts the Artificial Intelligence General Policy.

##### **Option 2:**

That Council does not adopt the Artificial Intelligence General Policy.

## **CONSIDERATIONS:**

### **Risk Management:**

The adoption of the AI policy will support Council in managing risks associated with AI technologies, including compliance with privacy legislation, data protection obligations and reputational risk.

It strengthens Council's risk management approach by:

- Requiring a formal risk assessment prior to the implementation of an AI solution and appropriate governance approval;
- Mandating human oversight controls and accountability for AI-driven outputs;
- Addressing risks relating to privacy, cybersecurity, bias and misinformation; and
- Prohibiting high-risk or unregulated uses of AI, including fully automated decision-making without oversight.

Effective implementation of the policy, supported by targeted training and ongoing capability development, will ensure risks are appropriately understood, managed and mitigated across Council.

### **Corporate and Operational Plans:**

The adoption of this policy strongly aligns with Council's strategic direction outlined in the Corporate Plan 2025–2030, by supporting greater effectiveness through strong governance, informed decision making and effective community outcomes.

This policy contributes to the Focus Area 5: Focused Council, by:

- Supporting informed, transparent and accountable use of AI systems;
- Establishing a contemporary governance framework for the use of emerging technologies; and
- Contributing to continuous improvement, innovation, learning, organisational capability and culture.

It also supports Council's Digital Transformation Agenda to accelerate public value creation to improve service delivery, enhance citizen engagement and modernise operations, while ensuring digital investments and initiatives remain strategically aligned with community needs and Council priorities.

Overall, the policy provides a foundation for the safe integration of AI into Council operations. It also reinforces Council's strategic objective of a focused, well-governed and forward-looking organisation, while also enabling innovation and supporting broader operational outcomes.

### **Statutory:**

The proposed policy ensures compliance with the relevant legislative frameworks. It also aligns with key frameworks such as the National Framework for the Assurance of AI in Government (2024), ensuring Council's approach is consistent with recognised Australian, Queensland and international standards and expectations.

**CONSULTATION:**

Consultation was undertaken during the development of the policy with relevant internal stakeholders, including Information Governance & Integrity, Organisational Development, Contracts and the Executive Leadership Team. The policy was also workshopped with Councillors.

**ATTACHMENTS:**

Attachment 1: Artificial Intelligence General Policy (#7749588)



Melvyn Pensee-Arnold  
Executive Manager Information & Technology Services



Lisa Whitton  
Chief Financial Officer

## ARTIFICIAL INTELLIGENCE (AI) POLICY

- Intent** This policy establishes guidance on the responsible, ethical, and strategic deployment of Artificial Intelligence (AI) technologies to drive operational excellence, improve service standards, and create sustained value for the community.
- Scope** It applies to all users including Councillors, employees, contractors, work experience personnel, volunteers, interns and third-party partners (including consultants), who use Council data and artificial intelligence technologies in their work for or in partnership with Cairns Regional Council (Council). The policy enables appropriate usage of AI within Council, whilst protecting data from unauthorised exposure.

## PROVISIONS

### 1. Introduction

Artificial Intelligence is currently driving transformation across all areas of government, industry and society. The technology offers unprecedented opportunities for Council to improve operational efficiency, enhance service delivery responsiveness and support data-driven decision making. This policy aims to facilitate the adoption of AI technologies at Council to serve the community, and sets out requirements for its ethical, safe, and compliant use, in line with Council's values, community expectations and legislative obligations.

### 2. Principles to guide the use of AI

The following AI principles have been developed with reference to the Australian Government's National Framework for the Assurance of AI in Government 2024 and are to be utilised to guide the design, development, deployment and use of AI technologies at Council.

The AI principles are organised into two distinct categories: Responsible and Strategic. This classification facilitates a clearer and more structured approach to managing the complexities linked with AI. The Responsible category addresses the overarching ethical objectives and societal values that AI support, while the Strategic category focuses on the operational, governance and practical aspects of implementing responsible AI.

#### 2.1 Responsible Principles

The responsible principles are foundational for the ethical, safe, and compliant use of AI, ensuring that AI systems are developed and deployed in ways that safeguard individuals, communities, and the environment.

The responsible principles must be complied with when using AI at Council:

- **Human, social and environmental wellbeing:** AI systems should promote human, social, and environmental well-being and facilitate respect for human rights, diversity, and individual autonomy.
- **Fairness:** All individuals should be treated fairly, without unfair discrimination. AI-driven decisions and outcomes should adhere to the same standards as human-made decisions, avoiding discrimination against individuals, communities, or groups.
- **Transparency:** AI systems must operate transparently, enabling their functioning and outputs to be understood, reproduced, and contested when necessary. People should be informed when interacting with AI systems in significant ways. Documentation regarding the use of AI technologies should be clear and detailed as required. When an AI system is employed in a significant way to generate information or make a decision, users are required to disclose its use.
- **Privacy and Security:** All systems incorporating artificial intelligence must uphold data security and operate in full compliance with applicable privacy and data protection legislation, as well as the policies, administrative instructions, and obligations of Council.
- **Reliability and Safety:** AI systems are expected to function reliably and consistently and in accordance with their intended purpose, without posing unreasonable safety risks. Suitable and proportionate safety measures must be established and maintained.
- **Contestability:** Whenever an AI system has a significant effect on individuals and their rights, community group or the environment, a timely and accessible process should be established to enable stakeholders to challenge the use or outcomes of the AI system.
- **Accountability:** Human oversight of AI systems is essential; therefore, a human-in-the-loop approach shall be employed. Subject matter experts must supervise AI systems throughout their lifecycle, identifying and considering technology, intended use, benefits, and risks.

## 2.2 Strategic Principles

The strategic principles are designed to support operational excellence and strong governance, which together promote ongoing success, adaptability, and trust in AI systems.

- **Continuous Monitoring and Improvement:** AI systems and related policies must be regularly reviewed and updated to reflect advances in technology, changes in law and regulations along with evolving community expectations.
- **Community Engagement:** Council will engage with the community about the use of AI in its services, providing accessible information and avenues for feedback and detection of AI issues.
- **Vendor and Tool Approval:** Only Council approved, and appropriately vetted AI Tools may be used. All third-party vendors must comply with Council privacy, security, ethical standards, and relevant Council policies and be subject to regular audit.
- **Human Centred Enablement:** AI technologies must be implemented as assistive tools that improve user efficiency and support informed decision-making. It does not replace human judgement, expertise, or accountability.

### **3. How Artificial Intelligence Will Be Used at Council**

#### **3.1 General Usage**

Council will implement and use AI technologies through a structured and deliberate approach to ensure:

- AI use is transparent and complies with all relevant data and privacy legislation, protecting personal and sensitive information of our employees, customers and the community, by implementing “privacy by design” and “security by design” principles.
- Risk assessments are conducted thoroughly before adopting any AI system to identify and mitigate risks to ensure suitable human oversight of the use of AI.
- Formal processes have been established to reduce bias, as well as the use of inaccurate or misleading information in decision-making.
- Internal users receive training to develop skills and understanding related to the use and implementation of AI.

As previously stated, users must only use Council approved AI tools for work purposes. A list of approved tools will be maintained by the Information and Technology Services Branch. Use of non-approved tools is prohibited to mitigate data residency and security risks.

#### **3.2 Data Protection and Security**

All actions, documents and data shared when utilising AI tools should be treated as disclosures of information and must adhere to Council's policies, including Confidential Information Management, Public Information Security and Management (including Intellectual Property), applicable legislation, and information privacy principles.

Council information must only be entered into public generative AI tools if it has already been released publicly or is deemed suitable for public disclosure. Users are responsible for all information that is shared or stored within AI tools and must not enter information which could enable public platforms to deduce sensitive or personal information through the aggregation of content over time.

Council will take advice from Australian Government and Queensland Government agencies regarding the use of AI systems and will block systems deemed an unacceptable risk.

#### **3.3 Unacceptable Usage**

Council will not utilise AI tools that:

- Compromise the privacy, security or rights of individuals, stakeholders or communities.
- Are deployed without a prior risk assessment and appropriate governance approval.
- Makes decisions, including fully automated “black box” AI determinations, that do not involve meaningful human oversight and have a substantial impact on individuals.
- Perpetuate or amplifies bias, discrimination or unfairness in decision making processes.
- Contravene any existing Council policies, administration instructions, or relevant legislation.
- Have had a mandatory direction issued by the Australian or Queensland State Governments, prohibiting the use of the solution.

#### 4. Roles and Responsibilities

To ensure effective governance and utilisation of AI systems, the table below outlines details the roles and responsibilities:

Roles	Overall Responsibility
Councillors	<ul style="list-style-type: none"> <li>Endorse the policy direction for use of AI technologies in Council.</li> <li>Follow the principles and guidelines outlined in this policy and any associated documents.</li> </ul>
Chief Executive Officer (CEO)	<ul style="list-style-type: none"> <li>Set overall strategy for AI adoption and governance within Council.</li> <li>Ensure guidance is provided to Councillors on the use of AI platforms.</li> </ul>
Executive Leadership Team (ELT)	<ul style="list-style-type: none"> <li>Oversee the implementation and adherence to this policy.</li> <li>Ensure the safe and ethical use of AI, by proactively identifying risks, protecting privacy and aligning with Council standards.</li> </ul>
Data Governance Panel	<ul style="list-style-type: none"> <li>Ensure that Council AI policies and procedures comply with legal, regulatory and ethical standards.</li> <li>Provide oversight and governance for AI usage.</li> </ul>
Information Governance & Integrity Unit	<ul style="list-style-type: none"> <li>Collaborate with Information and Technology Services, to ensure that AI use complies with legal, regulatory and ethical standards.</li> <li>Assist with regulatory assurance assessments.</li> <li>Provide support and guidance when requested.</li> </ul>
Information and Technology Services Branch	<ul style="list-style-type: none"> <li>Ensure the technical infrastructure supports secure and ethical AI use, including cloud computing, data storage and processing power.</li> <li>Provide strategic direction and technology leadership for Council's AI capabilities, ensuring AI adoption aligns with organisational goals, emerging best practices, and long-term ICT architecture.</li> <li>Assist with establishing operational processes to support the procurement and regulatory assessment of AI solutions.</li> <li>Provide technical support and guidance when requested.</li> </ul>
Organisational Development Unit	<ul style="list-style-type: none"> <li>Coordinate activities to build organisational capability and training for the ethical use of AI.</li> </ul>
Contracts Unit	<ul style="list-style-type: none"> <li>Coordinate updates to Council's procurement processes and contract templates, to ensure AI solutions are procured and implemented responsibly, ethically and securely.</li> </ul>
Associate Directors, Executive Managers	<ul style="list-style-type: none"> <li>Ensure AI solutions used within their area of responsibility are appropriately vetted, governed and</li> </ul>

Roles	Overall Responsibility
	monitored in line with policy requirements, including approvals, ongoing reviews, vendor oversight and stakeholder sign-off for public-facing use.
Users	<ul style="list-style-type: none"> <li>• Follow the principles and guidelines outlined in this policy and any associated documents.</li> <li>• Always check AI outputs to ensure that they are factual, reliable and unbiased.</li> <li>• Transparently disclose when an AI system is employed in a significant way to generate content or inform a decision for internal and external parties.</li> <li>• Complete any required AI training to understand the capabilities, limitations and risks of the AI systems they use.</li> <li>• Seek advice from Governance Unit or engage with the relevant subject matter expert within Council if unsure.</li> <li>• Are encouraged to use AI for productivity, provided it does not replace critical thinking or experience, and its application is appropriately disclosed.</li> <li>• Report any concerns or issues related to AI use to the relevant supervisor or Ethical Standards Unit.</li> </ul>

**5. Policy Compliance**

Compliance with this policy is critical to Council’s business and reputation. Non-compliance may result in Council and/or a user breaching relevant civil and criminal laws, which could result in substantial fines applying to Council and/or the user. Users should be aware Council reserves the right to monitor usage and verify compliance with this policy through various methods, including but not limited to monitoring usage, reviewing logs, accessing history and engaging internal and external audits.

**6. Definitions**

Reference Term	Definition
Artificial Intelligence (AI)	<p>Means a machine-based system that for explicit or implicit objectives, infers from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.<sup>1</sup></p> <p>Building on this definition, AI technologies enable computers to perform tasks that typically require human thinking, such as understanding information, making suggestions, or assisting decision-making, while supporting safe, ethical, and trusted outcomes, consistent with government policy. For the purpose of</p>

Reference Term	Definition
	this policy, the term AI refers to technologies such as Generative AI, Machine Learning, Natural Language processing and Computer Vision.
Artificial Intelligence Tools (AI Tools)	Software and applications that employ AI to generate or assist in generating content, solutions or decision-making processes.
Agentic AI	Agentic AI uses smart software “agents” that independently handle complex, multi-step tasks—like pulling data, analysing it, creating reports, and sending them—without constant human input. These systems work autonomously within clear boundaries, but always allow staff to review, approve, or override decisions. Because they can trigger actions across multiple systems, agentic AI requires strong governance around transparency, accountability, security, and human control.
AI Agent	<p>An AI agent is a software entity that operates within a defined digital environment, perceives state through data or events, reasons over goals and constraints, and autonomously executes actions via approved tools, applications, or systems to achieve specific objectives.</p> <p>AI agents are typically modular, combining capabilities such as planning, memory, decision logic, and tool invocation, and may use language models, rules, or other AI components depending on task scope and risk.</p>
Council	Refers to Cairns Regional Council.
Generative Artificial Intelligence	Often referred to as Gen AI, is a branch of artificial intelligence that focuses on the creation or generation of new content, such as text, images, voice, videos, software code, or other forms of data by leveraging algorithms, learning from data patterns, and machine learning techniques.
Personal Information	<p>Personal information encompasses a wide array of data or opinions that are capable of identifying an individual. The classification of information as personal depends on whether an individual can be identified, or is reasonably identifiable, given the specific circumstances.</p> <p><i>The Information Privacy Act 2009 defines personal information as:</i>  <i>‘Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion –</i>  <i>(a) Whether the information or opinion is true or not; and</i>  <i>(b) Whether the information or opinion is recorded in a material form or not.’<sup>2</sup></i></p> <p>Common examples include an individual’s name, signature, address, phone number, date of birth, bank account details, employment details, photograph, and commentary or opinions made by or about the individual.</p>
Public Generative Artificial Intelligence Tools	Any tool that is available to the public, takes user input and uses generative AI to create output. Examples include Gemini, ChatGPT (Open AI), Claude and Perplexity.
Sensitive Information	Sensitive information is personal information that includes information or an opinion about an individual’s:

Reference Term	Definition
	<ul style="list-style-type: none"> <li>• racial or ethnic origin</li> <li>• political opinions or associations</li> <li>• religious or philosophical beliefs</li> <li>• trade union membership or associations</li> <li>• sexual orientation or practices</li> <li>• criminal record</li> <li>• health or genetic information</li> <li>• some aspects of biometric information<sup>3</sup></li> </ul>

<sup>1</sup> Organisation for Economic Cooperation and Development (OECD) (2024) [Explanatory memorandum on the updated OECD definition of an AI system](#), OECD Artificial Intelligence Papers, No 8, OECD Publishing, Paris.

<sup>2</sup> Defined in Section 12, Information Privacy Act 2009 [Meaning of personal information](#)

<sup>3</sup> Defined in Schedule 5 Dictionary, Information Privacy Act 2009 [Meaning of sensitive information](#)

## 7. Related Council Governance Documents

### **General Policy**

Complaints Management  
 Management of Confidential Information  
 Public Information Security and Management (Including Intellectual Property)  
 Risk Management  
 Work, Health and Safety

### **Administration Instruction**

Acceptable Use of Information and Communications Technology and Services  
 Code of Conduct  
 Complaints Management Process  
 Information Security Management  
 IT Access for Non-Council Employees  
 Management of Intellectual Property Rights  
 Procurement Of Information and Communications Technology  
 Recordkeeping  
 Responsible Use of Artificial Intelligence (AI) Technologies  
 Websites and Mobile Apps

## 8. Relevant Legislation, Frameworks, Standards & Guidance

This Policy aims to ensure that permitted use of Council’s corporate information is consistent with relevant legislation, policy, and best practice.

### **Commonwealth Legislation**

- Copyright Act 1968
- Disability Discrimination Act 1992
- Privacy Act 1988
- Spam Act 2003

### **Commonwealth Frameworks/Standards/Guidance**

- National Framework for the Assurance of AI in Government 2024
- Policy for Responsible Use of AI in Government 2024 (Digital Transformation Agency)

**Queensland Government Legislation**

- Anti-Discrimination Act 1991
- Crime and Corruption Act 2001
- Criminal Code Act 1899
- Electronic Transactions (Queensland) Act 2001
- Human Rights Act 2019
- Information Privacy Act 2009
- Information Privacy and Other Legislation Amendment Act 2023 (IPOLA Act)
- Local Government Act 2009
- Public Records Act 2023
- Public Sector Ethics Act 1994
- Right to Information Act 2009

**International Standard/s**

- ISO/IEC 38507:2022 – Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organisations

**Queensland Government Guidance**

- Queensland Government’s Artificial intelligence governance policy (September 2024)
- Queensland Audit Office - Managing the ethical risks of artificial intelligence – Report 2: 2025-26 (24 September 2025)



**This policy is to remain in force until otherwise determined by Council.**

**Director Responsible for Review:**

**Chief Financial Officer**

**ORIGINALLY ADOPTED:** {Enter Date}

**CURRENT ADOPTION:** {Enter Date}

**DUE FOR REVISION:** {Enter Date}

**REVOKED/SUPERSEDED:** {Enter Date}

.....  
**Ken Gouldthorp**  
**CHIEF EXECUTIVE OFFICER**