

ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY

Purpose

To establish clear principles for the appropriate, ethical, and secure use of Artificial Intelligence (AI) tools by the City of Karratha. The policy ensures legal compliance, risk management, and community trust while enabling innovation through AI.

Scope

This policy applies to all Users—including Council Members, employees, volunteers, and contractors—who access or use the City’s information systems, data, or digital tools.

Definitions

- **Artificial Intelligence (AI):** Technology that mimics human intelligence to perform tasks including content generation, data curation, problem-solving, and learning from experience.
- **City:** The City of Karratha as the local government authority.
- **Confidential Data:** Organisational information that is sensitive, not for public disclosure, and may be owned or provided by third parties. *See also Council Policy CG-13 Confidential Information Policy.*
- **Contractor:** Any person or company engaged by the City to perform a service.
- **Council Member:** A currently serving elected member of the Council.
- **Elevated Risk:** As per the WA AI Assurance Framework; applies to AI systems that impact eligibility for services, automate impactful decisions, or process sensitive data.
- **Employee:** Any individual employed by the City on a full-time, part-time, or casual basis.
- **Generative AI:** A subset of AI that uses algorithms to generate new, original data, rather than working solely from pre-existing datasets.
- **Personally Identifiable Information (PII):** Information that can identify an individual, either alone or when combined with other data.
- **Public AI Applications:** Third-party AI tools that have not been risk assessed or contracted by the City.
- **Public Data:** Information lawfully made available to the public through official channels, posing no risk to privacy or confidentiality.
- **Sensitive Information:** Information that, if disclosed without authorisation, could cause harm to individuals or the organisation, including PII, legal advice, or security-related data.
- **User:** Any Council Member, employee, volunteer, or contractor using City data or information systems.

Policy Statement

The City recognises the benefits of using AI tools, in improving service delivery, operational efficiency, and decision support.

1. Ethical Use of AI

- AI tools must be used responsibly, ethically, and transparently.
- AI must support, not replace, human decision-making in critical or legally binding matters.
- All usage must adhere to applicable laws and City policies.

2. Compliance Requirements

- Users must comply with relevant legislation.
- Generative AI tools may only be used for work-related purposes and limited personal use, as defined in procedures.
- The use of generative AI tools must be done in accordance with OP-IT-01 IT Conditions of Use policy.

3. Privacy and Security

- City data may only be used in AI tools if it is publicly available or approved for release.
- No sensitive or confidential information (e.g., PII, legal documents) may be input into AI tools unless formally approved.

4. Transparency & Integrity

- All AI-generated content used in official documents or communications must include a disclosure statement.
- Users are responsible for reviewing and validating AI outputs before use.

5. AI in Decision-Making

- AI must not be used to make autonomous decisions such as recruitment, grants, procurement, development approvals, or compliance.
- AI may support research or preliminary analysis but final decisions must rest with authorised personnel.

6. Approved AI Tools

- Only tools listed in the **City's AI Tools Register** may be used for City business.
- Publicly available (free) tools may only be used with prior approval as outlined in the AI Usage Procedures.

7. Governance and Risk Management

- All new AI tools must be assessed for privacy, security, and ethical risk using the WA AI Assurance Framework. The Framework establishes a risk-based, ethics-aligned, whole-lifecycle approach to AI governance. The City will align with the Framework.
- "Elevated Risk" projects (e.g., those involving personal data or automated decision-making) require Human Rights Impact Assessment and governance review.

8. Training & Awareness

- All Users must complete AI awareness training prior to using AI tools and annually thereafter.

9. Incidents & Enforcement

- Misuse or unethical use of AI will be subject to investigation and potential disciplinary action.
- Incidents must be reported to designated managers as outlined in the procedures.
- The City reserves the right to monitor, audit, and review AI usage.

Roles and Responsibilities

Roles	Responsibilities
Chief Executive Officer (CEO)	Strategic oversight, approve policy exceptions
Director Corporate and Commercial Services (DCCS)	Approve AI tool use and risk assessments
Manager Information Technology (MIT) and ICT Team	Conduct risk assessments, maintain AI register, monitor incidents
Directors and Managers	Endorse business use cases, oversee compliance
Users	Use tools responsibly, complete training, report misuse

Related Documents

Legislation & Local Laws	<i>Freedom of Information Act 1992</i> <i>Public Sector Management Act 1994</i> <i>Local Government Act 1995</i> <i>Privacy Act 1988 (Cth)</i> <i>State Records Act 2000</i> <i>WA Privacy & Responsible Information Sharing 2024</i>
Relevant Delegations	
Strategies & Plans	
Related Council Policies	CG-13 Confidential Information Policy OP-IT-01 Conditions of Use of IT Facilities
Procedures, Documents & Forms	AI Usage Procedures (Companion Document) <i>Code of Conduct</i>

Policy Owner

Directorate	<i>Corporate & Commercial</i>
Department	<i>Information Services</i>

Review Management

Next review due:	<i>July 2026</i>
------------------	------------------

Version Management

Version	Date	Council Resolution #	Description
<i>1.0</i>	<i>July 2025</i>	<i>OCM250728-05</i>	<i>Original Policy Adopted</i>