DRAFT Governance/Service #:

1. Purpose

To establish organisational objectives and business rules for the ethical, secure, and responsible use of Artificial Intelligence (AI) technologies, including Generative AI, within the organisation. This policy ensures AI use aligns with privacy, security, transparency, and governance standards, while enhancing service delivery and operational efficiency.

2. Policy Statement

The City of Kalamunda (the City) is committed to the ethical, transparent, and responsible use of Artificial Intelligence (AI) technologies to enhance service delivery, improve operational efficiency, and support informed decision making. AI tools will be used to complement, not replace, human judgement and must always be applied with appropriate oversight, especially where outputs may impact the community or sensitive corporate functions.

3. Scope

This policy applies to all Council Members, employees, contractors, and volunteers using AI technologies in the course of their duties. It covers both commercial and publicly available AI platforms.

4. Definitions

Artificial Intelligence (AI): Technologies that perform tasks requiring human intelligence, such as decision-making, language processing, and automation.

Generative AI: AI that creates new content (e.g., text, images, audio) based on learned patterns. Examples being Copilot, ChatGPT.

Sensitive Information: Data that could compromise privacy or security if disclosed.

Public AI Platforms: Third-party AI tools not formally assessed or contracted by ICT Services.

Unapproved AI Platforms: AI tools that have been assessed or deemed inappropriate for Government use. Example being DeepSeek.

Bot: A software program that operates on the Internet and performs repetitive tasks.

Data Leak: Unauthorised disclosure of personal information, or loss of personal information.

5. Principles for AI Use

1. Privacy and Data Protection
   a. Use data anonymisation and informed consent.
   b. Do not input sensitive, confidential or personally identifiable information into AI platforms.

2. Security and Risk Management
    a. Use only approved AI platforms with no uncontrolled third-party data sharing.
    b. Conduct security assessments for all commercial AI tools.
    c. Prevent unauthorised access and ensure resilience against system manipulation.

3. Reliability and Accuracy
    a. AI outputs must be factually correct and free from bias.
    b. All outputs must be verified by a suitably qualified or experienced human before use in decision-making or public communication.

4. Transparency and Contestability
    a. Disclose AI use when it influences decisions, communications, or services.
    b. Maintain mechanisms for review and challenge of AI-generated outcomes.

5. Accountability
    a. Human oversight is mandatory.
    b. Maintain audit trails and assign clear responsibilities for AI use and outcomes.

6. Acceptable Use Guidelines

AI tools may be used:
For approved business related purposes on City owned devices.
For limited personal use on City owned devices that does not interfere with duties or compromise security in line with this policy.

AI tools must not be used:
To make decisions or deliver services without human oversight.
To upload sensitive or confidential data.
Without formal approval for public AI platforms.
To generate AI outputs that could result in harm, harassment, or the violation of ethical guidelines.

7. Approval and Use of AI Platforms

Public AI Platforms must undergo a security assessment by Information, Communications and Technology (ICT) Services.
Approval to use any AI platform must be granted by ICT Services.
Unapproved AI Platforms will be blocked for use where possible by ICT Services.

8. Roles and Responsibilities

Role	Responsibilities
CEO	Set strategic direction, approve exceptions, guide Council Members.
Directors	Oversee compliance, endorse procurement, escalate risks.
ICT Services	Governance, assesses tools, manages approvals, monitor the AI tools in use.
Business Unit Managers	Educate for policy compliance, support awareness.

Users	Use AI responsibly, verify outputs, protect data, report incidents.

9. Incident Reporting

Any incident involving data leakage, misuse, or unauthorised AI activity must be reported immediately to the ICT Services team and handled through the organisation’s incident management process.

10. Compliance and Monitoring

The City reserves the right to verify compliance through:

a) Usage monitoring
b) Log reviews
c) Browser history checks
d) Internal and external audits

Breaches may result in disciplinary action.

Status	Draft.		
Related Local Law	N/A		
Related Council Policies	Code of Conduct (Elected Members), Code of Conduct for Employees, Risk Management.		
Relevant Delegation	N/A		
Related Internal Procedures	ICT End User Security, ICT Security, Information Governance Framework, ICT Governance Framework.		
Related Budget Schedule	N/A		
Legislation	*Local Government Act 1995* *Local Government (Administration) Regulations 1996* *Freedom of Information Act 1992* *State Records Act 2000* *Public Sector Management Act 1994* *Commonwealth Privacy Act 1988* *WA Privacy and Responsible Information Sharing Act 2024 (PRIS)* *Western Australian Government Information Security Policy (WA-IS2)*		
Notes and Conditions	N/A		
Authority	Council		
Adopted		Next Review Date	