



USAGE OF ARTIFICIAL INTELLIGENCE POLICY

POLICY TYPE	DOCUMENT CONTROLLER	RESPONSIBLE MANAGER	POLICY ADOPTED	REVIEW DUE
Council	Strategic Innovation & Data Lead	Deputy CEO	25 May 2026	October 2027
PURPOSE	<p>This Policy explains how Council staff can use Artificial Intelligence (AI) safely and responsibly at work.</p> <p>It supports staff to use AI to save time, improve services, and help with decision-making, if a person checks the work.</p> <p>It also helps Council manage risks such as privacy breaches, data security issues, incorrect information, unfair outcomes, and damage to public trust.</p> <p>This Policy supports innovation while making sure AI use matches Council values, laws, community expectations, and Council's cyber security approach.</p>			
SCOPE	<p>This Policy applies to all Council employees, contractors, and consultants who use AI for Council work.</p> <p>It applies when people develop, buy, set up, use, or manage AI tools or AI features in other systems.</p> <p>AI can include tools that write or summarise text, analyse data, recognise images, or automate tasks (including generative AI and machine learning).</p> <p>This Policy applies whether the AI is built into Council systems, provided by a vendor, or accessed through external or cloud services.</p>			
DEFINITIONS	<p>For this Policy, these terms mean:</p> <p>Artificial Intelligence (AI) – Technology that allows computer systems to do tasks that usually require human thinking. This can include learning from data, predicting outcomes, recognising patterns, or generating content.</p> <p>AI Tool – Any software or service that uses AI to produce an output such as a summary, recommendation, prediction, or decision support. This includes AI features inside other systems and third-party AI services.</p> <p>Generative AI – A type of AI that creates new content such as text, images, audio, video, code, or data (for example, a tool that drafts text).</p> <p>Automated Decision-Making – When a system makes a decision without a person being involved. Under this Policy, automated decision-making that has legal, financial, regulatory, or significant personal impact is not permitted.</p>			

	<p>Human Oversight – When a person reviews AI outputs and can correct them, stop them, or override them. This keeps responsibility and judgement with Council staff.</p> <p>Approved AI Tool – An AI tool that Council has assessed and approved for use and recorded in the AI Tools Register.</p> <p>Unauthorised AI Tool – Any AI tool that Council has not approved for use with Council information, systems, or processes (including public or free tools used without approval).</p> <p>AI Tool Assessment Framework – Council's process for assessing AI tools before they are approved. Considerations include privacy, cyber security, data handling, intended use, decision impact, transparency, recordkeeping needs, vendor risk, and alignment with laws and policies.</p> <p>Information Classification – Council's way of sorting information by sensitivity and risk (for example Public, Internal, Confidential). Classification affects whether information can be used with a specific AI tool.</p> <p>AI Supply-Chain Risk – Risks from third-party vendors or components, including data residency, model training practices, security controls, subcontracting, and how incidents are reported.</p> <p>Explainability – How well an AI system's inputs, processing, and outputs can be understood and explained to decision-makers, affected people, auditors, or regulators.</p> <p>AI-Related Incident – Any real or suspected issue involving an AI tool, such as misuse, malfunction, privacy breach, or security breach that could affect Council operations, information, systems, staff, or the community.</p>
PRINCIPLES	<p>Council's use of AI is guided by these principles:</p> <ul style="list-style-type: none"> • Human, Social and Environmental Wellbeing – AI should benefit people, the community, and the environment. • Human-Centred Values – AI must respect human dignity, rights, and community values. • Fairness – AI must not treat people unfairly or create biased outcomes. • Privacy Protection and Security – AI use must protect personal, confidential, and sensitive information. It must not weaken Council's cyber security. • Reliability and Safety – AI systems must work as intended and be safe to use. • Transparency and Explainability – People should be able to understand when AI is used and how it supports an outcome. • Contestability – People must be able to question, challenge, and review AI-supported decisions. • Accountability – Council is always responsible for decisions, even when AI is used.

POLICY

Council may use AI to help with work tasks such as drafting text, summarising information, analysing data, automating routine tasks, improving services, and supporting planning and decisions.

AI must be used in a way that protects Council information and supports Council's cyber security and risk controls.

AI outputs must be checked by a person. Council staff remain responsible for the final work and decisions.

AI must not be used as the only basis for decisions that have legal, financial, regulatory, or significant personal impacts without appropriate human review and approval.

Supported Uses of AI

AI may be used for the following activities, as long as a person checks the result before it is used:

- Drafting, summarising, and editing documents and correspondence.
- Analysing data, identifying trends, and modelling scenarios.
- Automating routine tasks to improve efficiency.
- Supporting research, brainstorming, and developing options.
- Service improvement and innovation projects.
- Support learning, capability development and knowledge sharing to enhance workforce skills and understanding

All supported uses must follow this Policy and Council's cyber security and governance controls.

Prohibited Uses

AI must not be used for:

- Uploading, processing, or storing Council information in an unauthorised or unapproved AI tool or platform.
- Using information in AI tools when the information is classified above what that tool is approved to handle.
- Making automated decisions that significantly affect a person, without human oversight and authority.
- Creating content that is misleading, deceptive, discriminatory, or unlawful.
- By-passing Council security, procurement, governance, or approval processes.
- Any use that breaches legislation or Council policy.

Approved and Unauthorised AI Tools

Council will keep an AI Tools Register that lists AI tools that are approved for use. These tools will be assessed for privacy, security, data handling, and vendor/contract risks.

Staff must only use approved AI tools with Council information unless there is explicit approval to do otherwise.

Public, consumer, or free AI tools must not be used with Council information unless they are explicitly approved.

Staff must not assume that a publicly available AI tool meets Council privacy or cyber security requirements.

Contextual Considerations

Some AI uses are higher risk than others. Higher-risk uses may include activities that affect public rights, safety, surveillance, regulatory decisions, critical infrastructure, or major financial or reputational outcomes.

Before using AI, staff must consider:

- the sensitivity of the data being used (including information classification)
- the chance of bias or unfair outcomes
- whether the result can be explained and justified
- vendor and supply-chain risks (for example, data residency and subcontractors)
- the impact on the community and Council trust.

Higher-risk uses require a documented risk assessment and may require management or executive approval.

AI Tool Assessment Framework

Council will use an AI Tool Assessment Framework to assess AI tools and systems before they are approved or used.

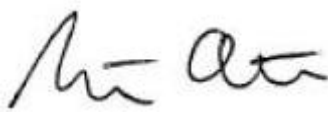
The assessment will consider privacy, security, information classification, cyber and supply-chain risk, intended use, decision impact, transparency and explainability, recordkeeping needs, and alignment with laws and Council policies.

The level of assessment will match the level of risk and the type of use.

Governance and Controls

Council will maintain governance and cyber security controls to support safe and responsible AI use, including:

- clear roles and responsibilities for AI oversight and cyber security oversight;
- risk, privacy, and impact assessments that match the risk level of the AI use and the sensitivity of the data;
- alignment with Council's information security, privacy, and data governance frameworks;
- checks on vendor and supply-chain risk (including data residency, subcontracting, model training practices, and incident notification);
- recordkeeping so Council can explain and show how AI was used (including auditability and RTI/FOI readiness); and
- ongoing monitoring, review, and continuous improvement of AI use.

	AI-related security, privacy, or misuse incidents must be reported and managed under Council's incident management and cyber security response processes.			
LEGISLATION AND RELATED DOCUMENTS	Internet & Digital Communication Use Policy Cyber Security Policy (Internal Council Policy) Records & Information Management Policy Personal Information Protection Policy Code of Conduct (Internal Council Policy) Communication and Media Policy <i>Personal Information Protection Act 2004</i> <i>Right to Information Act 2009</i> <i>State Service Act 2000</i> <i>Surveillance Devices Act 1991</i> <i>Evidence Act 2001</i> <i>Privacy Act 1988 (Cth)</i> <i>Australian Human Rights Commission Act 1986 (Cth)</i> <i>Administrative Decisions (Judicial Review) Act 1977 (Cth)</i> <i>Competition and Consumer Act 2010 (Australian Consumer Law)(Cth)</i> <i>Security of Critical Infrastructure Act 2018 (Cth)</i>			
ATTACHMENTS (IF APPLICABLE)	N/A			
STRATEGIC REFERENCE	5.6 Council has a modern, efficient and digital first approach			
MINUTE REFERENCE	26/82			
OFFICE USE ONLY	Update Register	Y	Training/Communication	Y
	Advise Document Controller	Y	Advise HR / MCO	Y
	Management Sign Off:  Date: 25 May 2026			