2.2.12 Artificial Intelligence (AI) Use

Type:	Office of the CEO
Legislation:	Privacy Responsibility and Information Sharing Act 2024 Information Commissioner Act 1924 State Records Act 2000 Local Government Act 1995 Freedom of Information Act 1992 Surveillance Devices Act 1998
Delegation:	Corporate Services
Other Related Document:	Information Classification Policy

Purpose

This policy establishes the principles, standards, and requirements governing the responsible use of Artificial Intelligence (AI) within the organisation. It ensures that AI technologies are used safely, ethically and effectively, and that risks associated with AI are appropriately managed. This policy must be read in conjunction with the Town's Information Classification Policy and prescribes how AI tools may be used according to the classification of information being shared.

Policy Scope

This policy applies to:

- All employees, contractors, consultants, third-party partners and Council Members
- All organisational systems, data, and devices
- Any AI-enabled tools, services, or workflows used in the course of work

Policy

Key Principles for the Use of AI

1. Ethical and Responsible Use

AI must be used in a manner consistent with the Town's values and ethical standards. Users must not generate or disseminate harmful, discriminatory or misleading content.

2. Privacy and Data Protection

AI tools must protect personal, confidential and sensitive information. Users must not enter information into any AI system unless that system is approved for the relevant classification of information.

3. Security and Risk Management

AI usage must not introduce cybersecurity vulnerabilities or expose the organisation to data loss, unauthorised access, or intellectual property risks.

4. Transparency

Users must be transparent when AI has been used to generate content, analysis or recommendations, particularly where accuracy, accountability or reliance on the output is significant.

5. Human Oversight

AI outputs must be reviewed by a human. AI must support—not replace—human judgement, decision-making, or accountability.

6. Compliance

All AI use must comply with applicable laws, regulations, contractual obligations, and internal policies.

Information Classification Labels

- **Unofficial** – information that is unrelated to the official work of the Town and would have no adverse impact on the Town if disclosed.
- **Official** – the default classification for most Town information created, received or used in the course of business where unauthorised disclosure may cause limited adverse impact to the Town.
- **Official Sensitive** – information that requires additional protection due to its sensitivity, including personal, legal, health, commercial-in-confidence or security-related information, where unauthorised disclosure may cause serious adverse impact to the Town, individuals or third parties, or may result in legal consequences.

Approved AI Application

AI use must align with the Town's information classification framework. Information classified as **Unofficial** or **Official** may be used in Microsoft Copilot and, where approved by the Executive Manager, Corporate Services, in other AI tools. Information classified as **Official Sensitive** must only be used in Microsoft Copilot and must not be entered into any other AI tool.

1. Microsoft Copilot

Microsoft Copilot is the Town's approved AI application for work-related use and is the only AI tool that may be used to input, process or analyse information classified as **Official Sensitive**. Other AI tools, including public chatbots and consumer-grade AI applications, may only be used where they have been approved by the Executive Manager, Corporate Services, and only for information that is not classified as **Official Sensitive**.

Rationale for Copilot as the Primary Approved AI Application

The organisation has approved Microsoft Copilot as the Town's primary AI application and as the only AI tool permitted for Official Sensitive information due to the following reasons:

1. Enterprise-Grade Security

Copilot is built on Microsoft's security and compliance framework, including:

- Enterprise authentication and access controls
- Data encryption in transit and at rest
- Integration with Microsoft 365 security and governance tools

This ensures that organisational data remains protected and never used to train public AI models.

2. Data Residency and Compliance

Copilot supports compliance with regulatory requirements, including data residency, auditability, and governance controls. This reduces legal and operational risks associated with AI use.

3. Integration with Existing Systems

Copilot integrates seamlessly with Microsoft 365 applications (Outlook, Teams, Word, Excel, PowerPoint, SharePoint), enabling:

- Secure productivity enhancements
- Consistent user experience
- Reduced operational complexity

4. Centralised Management and Monitoring

IT administrators can manage permissions, monitor usage, enforce policies, and apply security controls centrally—capabilities not available with consumer AI tools.

5. Reduced Risk of Data Leakage

Unlike public AI tools, Copilot:

- Does not store prompts or outputs outside the organisation's tenant
- Does not use organisational data to train external models
- Provides strict boundaries between corporate and public data

6. Vendor Trust and Support

Microsoft provides enterprise support, service-level commitments, and ongoing security updates, ensuring reliability and accountability

User Responsibilities

All users must:

- Use AI tools only for legitimate business purposes.
- Determine the classification of information in accordance with the Town's Information Classification Policy before entering it into any AI tool.
- Use Microsoft Copilot only when inputting, processing or analysing information classified as **Official Sensitive**.
- Only use other AI tools where they have been approved by the Executive Manager, Corporate Services, and only for information that is not classified as **Official Sensitive**.
- Not enter personal, confidential, commercially sensitive, legal, health or other **Official Sensitive** information into any AI tool other than Microsoft Copilot.
- Review AI-generated content for accuracy, appropriateness and compliance before use.
- Report any suspected misuse, data breach or security concern.
- Not use an in-private or incognito browser session to access Copilot.

Enforcement

Non-compliance with this policy may result in:

- Revocation of AI access privileges
- Disciplinary action
- Contract termination (for third parties)

Variation to this policy

This policy will be reviewed annually, or earlier if required due to changes in technology, regulation or organisational needs. The Town will notify employees of any variation to this policy by email.

Responsible Directorate:	Corporate Services
Reviewing Officer:	Executive Manager, Corporate Services
Decision making Authority:	Council
Policy Adopted:	16/6/26
Policy Amended/Reviewed:	