POLICY

Central Tablelands Water

ARTIFICAL INTELLIGENCE POLICY

DOCUMENT CONTROL

Document Title	Artificial Intelligence Policy
Policy Number	CTW-PR041
Responsible Officer	Executive Manager Corporate Services
Reviewed by	EMCS, General Manager
Date Adopted	30 April 2026
Adopted by	Council
Review Due Date	30 April 2027
Revision Number	1

Versions	**Date**	**Description of Amendments**	**Author**	**Review/ Sign Off**	**Minute No:** (if relevant)
1	17/12/2025	New policy	EMCS	Council	26/024

PURPOSE

To establish a framework for the use of Artificial Intelligence (AI) by Central Tablelands Water to ensure ethical, transparency, privacy and security implications are managed in ways that enhance operational effectiveness and collaboration.

SCOPE

This policy applies to all users, including staff, contractors, consultants and councillors. The policy enables the appropriate usage of AI internal and external-facing use, including content creation, document editing, and communication, while protecting data from unauthorised exposure.

POLICY STATEMENT

1. Key Categories of AI

- Generative AI (GenAI): Produces new content like text, images, or audio.
  - Example: CoPilot or Chat GPT for text generation, MidJourney for image generation
- Machine Learning (ML): Learns from data to predict outcomes or automate tasks.
  - Example: Analysing trends in asset deterioration
- Natural Language Processing (NLP): AI that interprets text to provide an output
  - Example: Summarising meeting minutes or translating documents
- Computer Vision: Analyses visual data for applications like asset inspection
  - Example: Identifying defects in concrete structures from photographs
- AI-Enhanced Productivity Tools: Tools that integrate AI for efficiency.
  - Example: CoPilot in Word or Excel
- Retrieval Augmented Generation (RAG): Reads defined documents to allow user interrogation
  - Example: NotebookLM

2. Approved Use of AI

AI may be used within the following approved cases:

- Drafting first versions of non-final documents, such as policy outlines, reports, briefings, or correspondence.
- Improving clarity, tone, structure, and conciseness of internally authored content.
- Generating or suggesting alternatives for plain English summaries.
- Preparing meeting notes or suggested minutes from input material.
- Brainstorming ideas for communications, campaigns, or service improvements.
- Internal research assistance (with human fact-checking).
- Machine Learning to help assess trends in data
- Computer vision for asset inspections
- CoPilot in Microsoft software to help develop documents or analyses

AI must not be used to:

- Make final decisions or official records.
- Generate or modify legally binding documents.
- Process sensitive, financial, health, confidential, or personal information.
- Operate without human oversight.

3. Principles for AI Use

The use of AI tools must align with these principles:

- **Human oversight**: All outputs must be reviewed and edited by staff before use or distribution. AI tools will be used to support, but not replace, human decision-making in critical areas.
- **Transparency**: AI-generated or AI-assisted content must be clearly acknowledged internally.
- **Privacy and Confidentiality**: No personal, sensitive, or confidential information may be entered into AI tools.
- **Accountability**: Staff remain responsible for the quality, accuracy, and appropriateness of all content created or edited using AI.
- **Equity and Inclusion**: AI tools should support communication that is inclusive, accessible, and free from bias.
- **Value for Public**: AI must create measurable public value through improved services, efficient operations, or strong community trust.
- **Explainability and Auditability**: all AI outputs must be explainable, traceable, and open to audit by internal or external stakeholders.

These Principles apply to all internal and externally sourced AI technologies and must be applied at all times, including during risk assessments, procurement processes, AI use case approvals, use and review.

4. AI Notetakers

CTW permits the use of AI notetakers of external meetings. All participants must accept the use of the AI notetaker in each meeting.

5. Data Use and Security

AI tools must use only AI platforms that have been vetted for data handling and privacy compliance.

The Generative AI tool approved by the CTW for Generative AI is Microsoft Co-Pilot. Staff MUST ENSURE they are logged into the Microsoft account prior to use. Any request to use other AI technology requires approval from the General Manager.

All access to AI technologies must comply with CTW's Information Technology Security and Information and Communication policies.

AI systems may only be accessed using CTW issued devices that meet CTW's security standards. The use of personally owned, unmanaged, or unapproved devices is strictly prohibited.

Where an AI system provides a setting to disable chat history, prompt retention or session logging, users must ensure that these features are turned off by default. Settings that allow model training using input data must always remain off. Auditability must be managed through CTW controlled logging tools and access records, not through third-party AI vendor history features.

AI systems used under this Policy form part of the CTW technology environment. In the event of AI security incidents, AI system failures, or unintended consequences, the Executive Manager Corporate Services and CTW's current IT Provider will initiate appropriate steps.

6. Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

- General Manager
  - Ensure staff understand appropriate AI use, monitor compliance, and provide training in AI use to staff.
- Staff
  - Use AI responsibly and in line with this policy.
  - Register all AI technologies used with CTW's Executive Manager Corporate Services
  - Document AI use where required.
- Councillors and External Parties
  - Use AI responsibly and in line with this policy.
  - Register all AI technologies used for CTW with the Executive Manager Corporate Services.
  - Document use where required.

7. Training and Awareness

All staff must complete training provided on:

- Responsible AI use
- Data security and privacy risks
- How and when to disclose AI use in their work.

POLICY REVIEW

This policy will be reviewed every 12 months or as required due to:

- Advances in AI technology
- Regulatory or legislative changes
- Feedback from internal or external users.

Staff are encouraged to suggest improvements or propose new AI use cases for consideration.

Any new use case is required to be subject to a formal Risk Assessment and Privacy Impact Assessment, such as NSW AI Assessment Framework, prior to being approved by the General Manager.

REFERENCES

- Australian Privacy Principles (Privacy Act 1988)
- AI Ethics Principles (Department of Industry, Science and Resources)
- Code of Conduct
- Information and Communication Technology Policy
- Information Technology Security Policy
- Records Management Policy

VARIATION

Council reserves the right to review, vary or revoke this policy.