AI Use Policy

Purpose

This policy sets out how RACI selects, deploys and governs Artificial Intelligence (AI) systems.

As RACI uses commercial, off the shelf AI systems, the policy focuses on safe, compliant use, privacy protection, and appropriate human oversight when interacting with third-party AI systems.

Scope

This policy applies to all RACI employees, contractors, and volunteers using AI tools in the course of RACI work, whether internally hosted or provided by third parties for RACI use.

Definitions

Artificial Intelligence (AI): Systems capable of generating content, analysing data, or making predictions or recommendations.

AI Tools (Off-the-Shelf): Commercial AI systems operated by third parties.

Generative AI: AI that creates new content (e.g. text, images, audio, video, or code).

Automated Decision-Making (ADM): Decisions substantially made by AI with limited human involvement.

Principles

AI must be used in ways that uphold accuracy, transparency, privacy, fairness, and integrity. All AI outputs require human review before use or publication.

AI Risk Classification

RACI classifies AI uses as Low, Medium or High risk based on impact to individuals, scientific integrity, legal obligations and reputational risk.

- Low: Internal drafting, summarisation of non-confidential materials, non-sensitive marketing concepts.
- Medium: Member communications, event operations, analytics on de-identified datasets.

- High: Any use that affects individuals' rights, involves personal or sensitive information, influences credentialling or safety, or constitutes Automated Decision Making (ADM).

Permitted Uses of AI

AI tools may be used for:

- drafting, editing and summarising content;
- generating non-sensitive marketing or design concepts;
- analysing non-confidential text, data analysis on de-identified or non-personal datasets;
- supporting administrative workflows such as transcription, scheduling.

Prohibited Use of AI

AI tools must not be used to:

- provide scientific, chemical, regulatory, or safety advice, including generating relevant instructions without expert human review and approval;
- make membership, credentialing, disciplinary decisions without human review and approval;
- generate assessments without expert human review and approval;
- process sensitive personal information without human review and approval;
- enter personal, confidential or sensitive information into publicly accessible generative AI tools or other systems;
- provide training or fine-tuning models on RACI held personal information without an approved PIA and CEO approval (RACI does not undertake model development);
- impersonate or mislead users about AI involvement;
- generate or disseminate fabricated scientific content, references or data;
- violate Australian law, RACI policies, contracts, or third-party rights.

Data Protection and Information Handling

Because off-the-shelf AI tools may process inputs externally, staff, contractors, and volunteers must:

- avoid entering personal or sensitive information into public AI models;
- only use AI tools approved by RACI;
- ensure outputs containing personal information (including incorrect "hallucinated" information) are treated as personal information under the Australian Privacy Principles (APP).

Vendor Due Diligence

RACI will only adopt AI tools after assessing:

- privacy and data-handling practices;
- security controls;
- data storage location and cross-border impacts;
- whether the tool uses prompts to train its models.

These expectations reflect the Office of the Australian Information Commissioner (OAIC) guidance for selecting commercially available AI products.

Human Oversight

All AI outputs must undergo human review for:

- accuracy and integrity;
- tone, bias, and reputational risk;
- compliance with laws, policies, and RACI standards.

Copyright and Intellectual Property

All staff, contractors, and volunteers must ensure AI generated content complies with copyright law, licensing terms, and RACI brand guidelines. Third-party confidential or IP protected information cannot be submitted, without relevant approval. All sources must be verified and attributed.

Recordkeeping, Audit and Monitoring

RACI will maintain records of approved AI tools, use cases and privacy assessments, with system-level monitoring and technical operations supported by its external managed services provider or third party vendors. Oversight remains with RACI.

Governance and Oversight

The day-to-day use and control of AI tools rests with the CEO.

High-risk uses require formal approval from the CEO, a completed Privacy Impact Assessment (PIA), and enhanced controls. PIA templates and other relevant guidance is available via the OAIC website.

RACI may rely on external providers for operational risk controls but retains accountability for compliance with the Privacy Act and APP.

Breaches of Policy

Misuse of AI tools may result in loss of access, retraining, disciplinary action, or reporting obligations under the Notifiable Data Breach scheme.

Approved by Board on	30 March 2026
Responsible Person	CEO
Scheduled Review	30 March 2028 (Once every two years, on date of Board approval)