

ASA Artificial Intelligence Policy

Document Control

Policy owner: Chief Executive Officer

Responsible Committee: Board

Approved by: Board of Directors

Effective from: 2 October 2026

Review due: 2 October 2027

Applies to: Directors, employees, contractors, consultants, volunteers, temporary staff and other workers performing work for, or on behalf of, ASA

Related documents: Code of Conduct; Privacy Policy; Whistleblower Policy; Delegations of Authority; Information Technology Policy.

Version: 1.0

1. Purpose

The purpose of this policy is to establish the principles and requirements governing the responsible, secure and effective use of artificial intelligence (AI) by the Australian Shareholders' Association (ASA).

ASA supports the responsible use of AI to improve productivity, research, education, communication and services to members.

ASA will use AI in a way that:

- supports ASA's purpose and strategic objectives
- maintains appropriate human judgement and accountability
- protects confidential, personal, commercially sensitive and security-sensitive information
- respects intellectual property, copyright and relevant regulations
- supports accurate and reliable communication and decision making
- maintains ASA's independence and integrity
- appropriately manages risks associated with AI.

AI is a tool to support people in their work. Accountability for ASA's decisions and activities remains with people.

2. Scope

This policy applies to ASA employees, directors, volunteers, consultants and contractors, and other ASA members who receive confidential or personal information from the Association when using AI for ASA-related activities.

AI includes generative AI tools, AI agents, machine learning systems, rule-based automation, predictive analytics and other technologies that generate content, recommendations or predictions, make decisions, or take actions using data.

An AI agent is an AI system capable of carrying out tasks or taking actions with a degree of autonomy, including interacting with software, systems or external services on a user's or ASA's behalf.

Standard spreadsheet formulas, conventional business intelligence tools and simple rule-based automation are not covered by this policy.

3. Principles

Human accountability

People remain accountable for work produced with the assistance of AI.

AI may support research, analysis and decision making, but material judgements and decisions must not be delegated solely to an AI system.

The person using AI is responsible for reviewing the resulting work and determining whether it is appropriate for its intended purpose.

AI-generated summaries or analysis must not substitute for a person's own review where they have responsibility for considering or approving the underlying material.

Accuracy and reliability

AI-generated information must not be assumed to be accurate.

Users must apply appropriate judgement and review to AI-generated work. Where accuracy is important, factual statements, quotations, calculations, company information and source references must be checked against reliable source material before being relied upon or published.

The level of checking should reflect the significance and potential consequences of the information.

Privacy, confidentiality and security

ASA information must be handled appropriately when using AI.

Confidential, personal, commercially sensitive or security-sensitive ASA information may only be entered, uploaded or processed using an AI system that ASA has approved for that type of information.

This includes, where applicable:

- personal information about members, employees or volunteers
- ASA intellectual property, proprietary content and unpublished material
- unpublished Board or committee information that is confidential
- confidential company engagement information
- commercially sensitive information from corporate partners or other organisations
- passwords, credentials or security information
- other information provided to ASA in confidence.

Existing ASA privacy, information security and confidentiality requirements continue to apply when AI is used.

Independence and integrity

AI must not compromise ASA's independence or the integrity of its work.

ASA's company monitoring, voting intentions, policy positions, advocacy and public commentary must remain grounded in evidence, independent assessment and appropriate human judgement.

AI may assist with the research and preparation of this work, but ASA's positions, voting intentions, recommendations and other material judgements must be determined by appropriately authorised people.

AI systems, vendors or commercial relationships must not determine or improperly influence ASA's positions or recommendations.

Transparency

ASA will be transparent about its use of AI where the nature or significance of that use makes disclosure appropriate.

AI must not be used to deceive, misrepresent or impersonate another person.

Fairness

AI should be used in a manner consistent with ASA's commitment to fair treatment, accessibility and inclusion.

Users should be alert to the possibility of bias, incomplete information or inappropriate assumptions in AI-generated outputs.

4. Use of AI Systems

Employees, directors, volunteers, members, consultants and contractors may use AI systems to assist with ASA work where appropriate.

AI may be used for activities such as:

- research using publicly available information
- drafting and editing
- summarising documents and publicly available information
- analysing and comparing information
- brainstorming and developing ideas
- administrative support
- data analysis where appropriate safeguards are in place
- preparation and analysis of internal business, management and financial reporting, subject to appropriate information safeguards
- preparation of educational and communication material
- improving internal processes and productivity.

Users must consider the sensitivity and significance of the information and activity before using AI.

Employees and directors must use AI systems approved by ASA for the handling of confidential, personal, commercially sensitive or security-sensitive information.

Confidential, personal, commercially sensitive or security-sensitive ASA information may only be entered, uploaded or processed using an AI system that ASA has approved for that type of information. This includes pasted text, attachments, screenshots, meeting recordings and allowing an AI assistant to access email or cloud storage.

Any confidential or sensitive information must not be entered into an unapproved AI service, whether free or paid. Turning off model training, using a temporary chat or deleting a conversation does not constitute ASA approval. Removing names is insufficient where a person can still be identified or the remaining material is confidential.

ASA may restrict particular AI systems or uses where necessary to manage privacy, security, legal, intellectual property or reputational risks.

5. Higher-Risk Use

Additional care and human oversight are required where AI is used for work that could materially affect ASA, its members or external stakeholders.

This may include:

- unpublished policy positions and submissions
- member lists
- analysis of member or stakeholder information
- significant unpublished public statements (including Voting Intentions and pre-AGM meeting notes)
- material business, financial or Board reports
- decisions affecting individual members, employees or volunteers, or candidates for ASA positions
- analysis that could materially influence a significant ASA decision
- activities involving sensitive, confidential, personal, commercially sensitive or security-sensitive information.

For these activities, AI-generated material must be reviewed by an appropriately knowledgeable person before it is relied upon, approved or published.

Where a proposed AI use presents material privacy, security, legal, intellectual property, reputational or governance risks, it must be referred to the CEO before implementation.

6. AI Agents and Automated Actions

AI agents that can take actions on behalf of ASA require appropriate approval and oversight before use.

The level of human oversight must reflect the potential consequences of the actions the agent can take.

AI agents must not autonomously make material decisions, enter into commitments or transactions, approve expenditure, publish significant external communications, exercise voting rights, or access or disclose confidential, personal, commercially sensitive or security-sensitive information unless specifically authorised with appropriate controls in place.

A person must remain accountable for the use of an AI agent and, where appropriate, be able to review, stop or override its actions.

7. Intellectual Property and Copyright

Users must respect intellectual property and copyright when using AI.

ASA copyright material, proprietary content or other intellectual property must not be uploaded to an AI system where doing so could compromise ASA's ownership, confidentiality or rights in that material.

Copyright material or intellectual property belonging to third parties must not be uploaded, reproduced or used through AI in a way that may infringe the rights of the owner.

Users must not assume that AI-generated material is original or free from third-party intellectual property rights. Material intended for significant external publication or commercial use must be appropriately reviewed before use.

Where AI is used to develop material for ASA, appropriate steps must be taken to ensure ASA can use, reproduce and publish the resulting material as intended.

8. Prohibited Use

AI must not be used to:

- make material decisions on behalf of ASA without appropriate human involvement
- enter confidential, personal, commercially sensitive or security-sensitive information into an AI system that has not been approved for that type of information
- deliberately create false, deceptive or misleading information
- impersonate another person without appropriate authority
- circumvent ASA policies, security controls or legal obligations
- publish or rely on material AI-generated content without appropriate human review
- make decisions about individuals where doing so could result in unfair or discriminatory treatment
- infringe ASA's or another party's intellectual property rights.

9. Governance and Responsibilities

The Board is responsible for approving this policy and overseeing ASA's approach to the governance of artificial intelligence.

The CEO is the policy owner and is responsible for overseeing implementation of the policy and ASA's approach to responsible AI use. The CEO will ensure there is an AI register, monitoring, stakeholder feedback and disclosure arrangements.

ASA will identify AI systems approved for handling confidential, personal, commercially sensitive or security-sensitive information and any conditions applying to their use.

Before ASA adopts an AI system that will handle such information, appropriate consideration must be given to its privacy, security, data handling, contractual terms and other material risks.

Managers are responsible for supporting appropriate AI use within their areas of responsibility.

All employees, directors, volunteers and contractors covered by this policy are responsible for:

- complying with this policy
- protecting ASA information
- applying appropriate judgement when using AI
- checking AI-generated outputs to an appropriate standard
- completing relevant training where required
- reporting either minor or significant errors, incidents or concerns involving AI.

10. AI Incidents

Significant AI-related incidents, suspected material errors or suspected breaches of this policy must be reported promptly to the relevant manager or the CEO.

The CEO or delegate may pause further distribution of suspected errors where continued reliance could cause harm. A knowledgeable person may be assigned to establish the facts against original sources and identify any affected publications and decisions.

For company monitoring materials, the responsible monitoring lead should verify the correction.

In the case of confidentiality incidents, the nature and extent of the disclosure should be assessed, and reasonable steps taken to determine whether the incident constitutes an eligible data breach under the Privacy Act and requires notification under the Notifiable Data Breaches scheme.

Depending on the circumstances, ASA may suspend or restrict the use of an AI system while an incident is investigated.

The Chair should be advised of significant incidents.

Lessons from incidents should be considered when updating systems, processes, training and this policy.

11. Training and Guidance

ASA will provide appropriate guidance, as required, to employees, directors and relevant volunteers, contractors and consultants on the capabilities, limitations and risks of AI, and ASA's policy of working with AI. This will be incorporated into induction procedures and the conditions attached to access to confidential materials.

Training and guidance will be proportionate to people's responsibilities and the nature of their AI use.

Practical Guidance

Situation	Practical option
Research involving public, non-personal information	Use a permitted public AI service, subject to copyright requirements and appropriate checking of outputs.

Help with structure, wording or drafting	Use generic, fictional or de-identified examples without uploading confidential, personal or commercially sensitive information.
Work involving confidential, personal, commercially sensitive or security-sensitive information	Use an ASA-approved AI system for that type of information or seek assistance from an authorised person using such a system.
No approved AI access is available for the information involved	Do not use an unapproved AI service. Complete the task without AI assistance or seek assistance from an authorised person.

12. Policy Review

This policy will be reviewed at least every year.

An earlier review may be undertaken following:

- a significant AI-related incident
- a material change in ASA's use of AI
- significant developments in AI technology
- changes to relevant laws, regulations or recognised standards.