



Artificial Intelligence (AI) Policy

[MONTH 2026]

TEMPLATE ONLY





[THIS PAGE IS INTENTIONALLY LEFT BLANK]

TEMPLATE





Contents

Artificial Intelligence (AI) Policy	1
1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	5
5. Data Protection and Privacy	5
6. Intellectual Property	5
7. Training and Awareness.....	6
8. Policy Compliance	6
9. Related Standards, Policies and Processes	6
10. Revision History	6





1. Introduction

Artificial Intelligence (AI) tools are increasingly used to support productivity, decision-making, and service delivery across organisations. The rapid evolution of these technologies, particularly generative AI, presents significant opportunities to improve efficiency and innovation.

However, the widespread adoption of AI also introduces heightened risks, including data leakage, loss of intellectual property, inaccurate or biased outputs, regulatory non-compliance, and reduced visibility over how organisational data is processed and stored. These risks are amplified by the growing use of publicly accessible AI platforms and the potential for uncontrolled or “shadow AI” usage within business environments.

This policy establishes a framework to ensure that AI is used in a controlled, secure, and responsible manner. It is designed to align AI usage with [Company Name] operational requirements, legal obligations, and commitment to maintaining client trust and data security.

2. Purpose

The purpose of this policy is to define the minimum requirements for the appropriate, ethical, and secure use of Artificial Intelligence tools within the organisation. This policy aims to:

- Support the responsible and secure adoption of AI technologies
- Protect sensitive, confidential, and personal information from unintended exposure
- Ensure appropriate human oversight, accountability, and decision-making
- Reduce operational, legal, and reputational risks associated with AI usage
- Maintain trust with clients, partners, and stakeholders.

3. Scope

This policy applies to:

- All employees, contractors, consultants, and third parties acting on behalf of [Company Name]
- All Artificial Intelligence tools and systems used for organisational purposes, including publicly available and enterprise-grade platforms
- All use of AI across business activities, including administration, service delivery, technical operations, communications, research, and decision-making.





4. Policy

- 4.1 AI tools may be used to support organisational objectives and improve operational efficiency, provided such use complies with this policy and all relevant standards and obligations.
- 4.2 AI must be treated as an assistive technology and must not replace human judgement, particularly in situations where decisions may impact individuals, services, clients, or organisational outcomes.
- 4.3 All outputs generated by AI must be critically assessed for accuracy, appropriateness, and potential bias prior to use or distribution. Employees must not rely solely on AI-generated outputs without validation.
- 4.4 The use of AI tools must not result in the disclosure of sensitive, confidential, or client information to unapproved systems. Employees must exercise caution when entering any data into AI platforms and ensure that data classification and security requirements are always maintained.
- 4.5 AI must not be used to generate misleading, deceptive, discriminatory, or harmful content, nor should it be used in a manner that could damage the organisation's reputation or breach legal obligations.
- 4.6 The use of AI for fully automated decision-making that impacts individuals is strictly prohibited unless appropriate human oversight, review, and approval mechanisms are in place.
- 4.7 Any new, high-risk, or business-critical use of AI must be reviewed and approved by management prior to implementation to ensure that risks have been appropriately assessed and mitigated.

5. Data Protection and Privacy

- 5.1 The use of AI tools must comply with all applicable data protection and privacy requirements.
- 5.2 Sensitive, confidential, or personal data must not be entered into public or unapproved AI tools. Where AI usage is required for business purposes, only approved platforms that meet organisational security and compliance requirements may be used.
- 5.3 Wherever possible, anonymised or de-identified data should be used to minimise risk exposure. Users must remain aware that some AI tools may retain, process, or reuse data outside the organisation's control.
- 5.4 All AI-related data handling must comply with relevant legislation (including the Privacy Act and other applicable regulations) and align with **[Company Name]** internal privacy and information security policies.

6. Intellectual Property

- 6.1 AI-generated content must be reviewed to ensure it does not infringe on copyright, trademarks, confidential information, or other intellectual property rights.
- 6.2 Responsibility for the accuracy, legality, and appropriateness of all final outputs remains with the individual using the AI tool.
- 6.3 Where AI has materially contributed to content or deliverables, consideration should be given to whether disclosure is appropriate, particularly in client-facing or regulated scenarios.





7. Training and Awareness

[Company Name] will promote awareness of responsible AI use and provide guidance or training where appropriate.

Employees are expected to maintain an understanding of AI-related risks, including data security, privacy, and regulatory considerations, and to apply this knowledge in their day-to-day activities.

Staff are encouraged to raise questions or concerns regarding AI usage with management, particularly in situations where risk or uncertainty exists.

8. Policy Compliance

8.1 Compliance Measurement

Compliance with this policy may be verified through periodic reviews, audits, system monitoring, and management oversight to ensure appropriate and secure use of AI technologies.

8.2 Exceptions

Any exception to this policy must be formally approved in advance by management and documented appropriately.

8.3 Non-Compliance

Any individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or engagement.

9. Related Standards, Policies and Processes

- Privacy Policy
- Information Security Policy
- Code of Conduct

10. Revision History

This policy will be reviewed periodically to ensure it remains aligned with evolving AI technologies, emerging threats, and regulatory developments.

