# AI Usage & Ethics Policy Template

## For Small, Mid & Medium‑Sized Australian Businesses

*Version 0.9 – June 2025*

### 1  Purpose

This Policy sets out our organisation’s commitment to use Artificial Intelligence (AI) in a way that **drives innovation, productivity and customer value creation first**, while safeguarding people, society and the environment. It embeds Australia’s AI Ethics Principles, the 2024 Voluntary AI Safety Standard guardrails, relevant provisions of the *Privacy Act 1988* (as amended), and ISO/IEC 42001:2023.

### 2  Scope

* Applies to **all employees, contractors and third‑party providers** who design, develop, procure, deploy or manage AI systems on behalf of .
* Covers AI or Automated Decision‑Making (ADM) technologies that influence internal operations, employee processes or external products/services.

### 3  Definitions

| Term | Meaning |
| --- | --- |
| **AI System** | Software that performs tasks normally requiring human intelligence by learning patterns, generating content or making decisions. |
| **High‑Risk AI** | Any AI that can materially affect customers’ finances, health, safety, legal rights or employment. |
| **AI Registry** | Our internal inventory of all AI systems and their risk tier, owner and safeguards. |
| **AI Ethics & Innovation Committee (AEIC)** | Cross‑functional body that oversees policy compliance, risk assessments and use‑case approvals. |

### 4  Guiding Principles

1. **Innovation & Customer Value** – Deploy AI to create new value propositions before focusing on cost cutting.
2. **Human, Societal & Environmental Wellbeing** – AI must benefit people and planet.
3. **Human‑Centred Values** – Respect autonomy, dignity, diversity and human rights.
4. **Fairness & Inclusion** – Identify and mitigate bias; ensure equitable outcomes.
5. **Privacy & Security by Design** – Comply with the *Privacy Act 1988* and OAIC guidance; protect data integrity and confidentiality.
6. **Transparency & Explainability** – Clearly disclose AI use to affected stakeholders and be able to explain significant decisions.
7. **Reliability & Safety** – Test, validate and monitor AI to operate as intended.
8. **Accountability & Governance** – Define clear roles; maintain auditability; enable contestability.

### 5  Policy Statements

#### 5.1 Innovation & Productivity for Growth

* AI initiatives must state how they **create new revenue, improve customer experience or lift productivity**.
* Pure cost‑cutting initiatives that risk disproportionate job losses will be **deprioritised** unless accompanied by clear value‑creation justification.

#### 5.2 Employee Collaboration

* Employees at all levels may propose AI ideas via the **AI Use‑Case Portal**.
* Each project team must include **front‑line employee representatives** during design and testing.

#### 5.3 Use‑Case Selection Criteria

An AI proposal will proceed only if it:

1. Aligns with strategic goals for growth and innovation;
2. Passes an **AI Risk & Ethics Assessment** (Appendix B);
3. Demonstrates stakeholder benefits outweigh risks;
4. Provides measurable KPIs and monitoring plan.

#### 5.4 Risk Assessment & Compliance

* All High‑Risk AI requires **Algorithmic Impact Assessment (AIA)**, Privacy Impact Assessment (PIA) and approval by the AEIC.
* AI Registry must be kept current; risk tier updates at least annually.

#### 5.5 Bias Mitigation & Fairness

* Data sets must be assessed for representativeness and bias.
* Models impacting employment, credit, health or pricing must undergo independent fairness testing.

#### 5.6 Privacy & Data Protection

* Personal or sensitive information shall only be used consistent with consent, purpose limitation and data minimisation principles.
* No personal data may be entered into public generative AI tools without AEIC approval and documented safeguards.

#### 5.7 Human Oversight & Control

* High‑impact decisions always retain a **human‑in‑the‑loop** or **human‑on‑the‑loop** override.
* Contestability: Individuals can request a human review of any significant AI decision.

#### 5.8 Employment Impact & Workforce Transition

* Where AI adoption may change roles, the company will **prioritise up‑skilling, re‑skilling and redeployment**.
* In the rare event redundancies are unavoidable, the company commits to transparent consultation, fair separation terms and support programs.
* Employees are expected to support such transitions **provided the spirit of this Policy – value‑creation before cost‑cutting, fairness and collaboration – is demonstrably upheld**.

### 6  Governance Structure & Responsibilities

| Role | Key Duties |
| --- | --- |
| **Board / Executive** | Endorse Policy, set appetite for AI risk, review annual AI Ethics Report. |
| **AEIC** | Maintain AI Registry, approve high‑risk use cases, oversee audits, publish guidance. |
| **Business Owners** | Submit use‑case proposals, ensure compliance in their domain. |
| **IT & Data Leaders** | Implement technical safeguards, data governance, security controls. |
| **HR / People & Culture** | Manage workforce transition, training and change‑management. |
| **All Employees** | Use AI responsibly, report concerns, engage in continuous improvement. |

### 6.1  Employee Obligations

To ensure AI systems are used safely and reliably across technical disciplines, **every employee** must:

* **Validate engineering outputs** – Cross‑check any AI‑generated calculations, designs or ratings via manual methods and peer review in line with Engineers Australia Practice Note 01.
* **Verify research insights** – Corroborate AI‑derived research findings or market data with at least **two authoritative sources** before using them in decision‑making or client deliverables.
* **Engage in QA/QC** – Participate in testing cycles by supplying representative data samples, completing accuracy checklists and logging anomalies for AEIC review.
* **Document assumptions & limitations** – Clearly record AI model parameters, data provenance and any known uncertainties in project files.
* **Escalate concerns** – Promptly flag irregular, biased or unsafe outputs via the Incident Response channel.
* **Follow supporting SOPs** – Adhere to engineering, research and QA/QC Standard Operating Procedures (SOPs) that provide step‑by‑step checks before sign‑off.

### 6.2  Responsible Personal Use of AI & LLM Tools

Employees are encouraged to explore public or commercial Large‑Language Models (LLMs) and other AI tools **for learning, ideation and productivity**, provided they:

* **Stay lawful & ethical** – No generation or distribution of unlawful, defamatory, discriminatory, hateful, violent or sexually explicit content.
* **Protect confidentiality** – Do **not** input client data, personal information, designs, source code or commercially sensitive material into any external AI service unless it is on the **company‑approved list** and covered by a data‑processing agreement.
* **Align with IT Acceptable Use** – All use must comply with the organisation’s IT Acceptable Use Policy and Code of Conduct. Any breach will trigger disciplinary procedures.
* **Attribute & verify** – Clearly mark AI‑assisted content and **fact‑check** before internal or external circulation. Critical communications (marketing, legal, contractual) require manager review.
* **No automated outreach** – Employees must not deploy AI chatbots or mass‑email agents that contact external parties without AEIC authorisation and compliance checks (e.g., Spam Act suppression lists).
* **Respect intellectual property** – Refrain from prompting AI to reproduce copyrighted material; cite sources when re‑using AI‑generated outputs.

### 7  Operational Procedures

1. **AI System Register** – Mandatory entry before procurement or build.
2. **Use‑Case Proposal Workflow** (Appendix A) – Idea → Preliminary AIA → AEIC review → Pilot → Full deploy.
3. **Testing & Validation** – Pre‑launch bias tests, performance metrics, security review.
4. **Monitoring & Feedback** – Real‑time alerts for drift; quarterly review meetings; user feedback loop.
5. **Incident Response** – Follow Cyber‑Security Incident Plan; notify AEIC and legal within 24 hrs of any AI malfunction or data breach.

### 8  Training & Awareness

* Annual **Responsible AI training** is mandatory for all staff; role‑specific deep dives for developers and data scientists.
* Regular lunch‑and‑learns showcase successful employee‑led AI innovations.

### 9  Transparency & Communication

* Public‑facing **AI Disclosure Statement** summarises key AI systems and safeguards.
* Privacy Policy updated to meet OAIC recommendations on automated decisions.

### 10  Review & Audit

* Internal audit of AI Registry and high‑risk systems at least **every 18 months**.
* Policy reviewed **biennially** or sooner if regulatory changes require.

### 11  References & Related Documents

* Australian Government AI Ethics Principles (2019)
* Voluntary AI Safety Standard (2024) – 10 Guardrails
* *Privacy Act 1988* & OAIC AI/Privacy Guidelines (2024)
* ISO/IEC 42001:2023
* NSW Government AI Ethics Policy (2023)

### 12  Document Control

| Version | Date | Author | Approved By | Notes |
| --- | --- | --- | --- | --- |
| 0.0 |  |  | – |  |

### Appendices

**Appendix A – AI Use‑Case Proposal Form**
*Project title, Sponsor, Problem Statement, Expected Value, Stakeholders, Data Sources, Risk Tier, KPI, Resources, Employee Representatives.*

**Appendix B – AI Risk & Ethics Assessment Checklist**
*Risk Tiering, AIA Summary, Bias Testing Results, Privacy Impact, Security Controls, Human Oversight Plan, Compliance Yes/No.*

**Appendix C – Stakeholder Communication Template**
*Plain‑language explanation of AI system, benefits, any impact on roles, contact for questions.*

*This template is for guidance only, it is the sole responsibility of the end user to modify and adjust for their own business requirements, and to ensure it complies with all legal business requirements, under which the company operates.*