



Policy Name:	Artificial Intelligence Usage Policy
Attention:	LSH Group Australia Employees
Version:	1.0
Last Reviewed:	1 st April 2026
Effective From:	1 st April 2026
Approved By:	GCEO / Corp Review / MD

Artificial Intelligence Usage Policy

1. Purpose

This policy sets out the requirements for the responsible, ethical, and lawful use of Artificial Intelligence ("AI") tools and technologies within LSH Group Australia ("the Group"). The purpose of this policy is to ensure AI is used to enhance operational efficiency, decision-making, and customer service while maintaining data security, privacy, transparency, accuracy, and compliance with applicable Australian laws and regulatory guidance.

The Group supports the responsible use of generative AI systems where such systems are approved by the Group (currently Microsoft Copilot) and used strictly in accordance with this policy and other applicable Group policies.

2. Scope

This policy applies to all employees, contractors, labour hire personnel, consultants, officers, and representatives of the Group (collectively, "Workers") who use, access, develop, procure, or interact with AI systems in any capacity, including but not limited to:

- Sales, marketing, and customer engagement tools;
- Human Resources, recruitment, performance management, and learning systems;
- Service department applications, diagnostics, forecasting, and reporting tools;
- Administrative, communication, finance, and data analytics tools.

3. Legislative and Regulatory Framework

Use of AI must comply with all applicable Australian laws, standards, and regulatory guidance, including but not limited to:

- *Privacy Act 1988 (Cth)* and the Australian Privacy Principles (APPs);
- *Spam Act 2003 (Cth)* (for AI-assisted marketing and communications);
- *Fair Work Act 2009 (Cth)* and anti-discrimination legislation;
- *Work Health and Safety Acts and Regulations* (Cth and State-based);
- Intellectual property and copyright laws (including the *Copyright Act 1968 (Cth)*);
- OAIC guidance on AI, privacy, and automated decision-making;
- Any applicable contractual, confidentiality, or regulatory obligations.

4. Acceptable Use of AI

AI tools may be used to support legitimate business activities provided that the following principles are met:

4.1 Accuracy and Human Oversight



- AI-generated outputs (including emails, reports, recruitment materials, marketing content, summaries, analyses, or recommendations) must be reviewed, verified, and approved by a responsible employee before being relied upon, published, or distributed.
- AI must not be used as the sole basis for decisions that have legal, safety, financial, or significant people impacts.

4.2 Privacy and Data Protection

- Personal information, sensitive information, or confidential business information must not be entered into public or unapproved AI platforms.
- Any handling of personal information using AI must comply with the APPs, including requirements relating to collection, use, disclosure, data security, and overseas data transfers.

4.3 Compliance and Lawful Use

- AI must only be used in ways that comply with Group policies, Australian law, and regulatory obligations.
- AI must not be used to circumvent internal controls, approval processes, audit requirements, or security safeguards.

4.4 Transparency

- Workers must not represent AI-generated content as entirely human-created where accuracy, authorship, or source integrity is material.
- Workers must disclose to their Manager, and where appropriate to customers or stakeholders, when AI tools have materially contributed to work outputs.

4.5 Accountability

- Workers remain fully accountable for all work products created with the assistance of AI.
- Responsibility for accuracy, compliance, fairness, and appropriateness cannot be delegated to an AI system.

5. Unacceptable Use of AI

Workers must not use AI systems to:

- Generate, promote, or disseminate misleading, deceptive, discriminatory, defamatory, or otherwise inappropriate content;
- Undertake automated decision-making that affects employment, safety, remuneration, performance management, or legal rights without appropriate human review and approval;
- Upload or disclose confidential, proprietary, commercially sensitive, or regulated information to public or consumer-grade AI tools (e.g. ChatGPT, Google Gemini) unless expressly authorised;
- Infringe copyright, intellectual property rights, or licence conditions;
- Breach contractual commitments to customers, suppliers, or business partners;
- Create or use AI outputs in a manner that could reasonably cause harm to individuals, customers, or the Group.

6. Data Security and Confidentiality



- All data entered into AI systems must comply with the Group's Privacy Policy, Information Security Policy, and Internet, Email and Computer Usage Policy.
- Sensitive or confidential data may only be processed using AI systems approved by IT and Compliance.
- Public or consumer-grade AI tools must not be used to store, analyse, or train on Group data unless formally authorised.

Permitted Data Categories

Only the following data may be used in AI systems without additional approval:

- Publicly available data not subject to legal or contractual restrictions;
- Non-confidential, non-personal business data;
- Synthetic or anonymised data that cannot reasonably identify an individual.

7. Employee Responsibilities

Workers must:

- Use AI ethically, responsibly, and in accordance with this policy;
- Clearly disclose AI usage in their work to Managers and relevant stakeholders;
- Independently verify and fact-check AI outputs before reliance;
- Ensure AI-assisted work is reviewed by an appropriately senior professional who is aware that AI was used;
- Report suspected misuse, bias, security incidents, or data breaches immediately to a Manager or IT;
- Complete mandatory AI, privacy, and data protection training;
- Obtain prior approval before uploading or sharing confidential, proprietary, or regulated data;
- Review AI system terms of use to confirm commercial use rights and ownership of outputs;
- Consider security, privacy, and data residency risks before using any AI system;
- Protect login credentials and never share passwords or access details;
- Not use AI in any way that could damage the Group's reputation or legal position.

8. Management Responsibilities

Managers must:

- Ensure team awareness of and compliance with this policy;
- Approve AI tools in consultation with IT, Legal, and Compliance;
- Monitor AI usage for legal, ethical, and operational risk;
- Ensure appropriate training and guidance is provided;
- Escalate high-risk or novel AI use cases for further review.

9. Ethical Use and Risk Management

9.1 AI Risk-Tiering Framework

The Group adopts a risk-based approach to the use of AI systems. AI use cases are classified as Low, Medium, or High risk based on their potential impact on individuals, legal rights, safety, compliance, and the Group's reputation. The table below provides guidance only and does not remove the requirement to seek approval where uncertainty exists.



Risk Tier	Description	Examples of Use Cases	Approval & Controls Required
Low Risk	AI use with minimal impact, no personal information, and no material legal, safety, or people implications. Outputs are informational or assistive only.	• Drafting internal emails or presentations • Summarising non-confidential documents • Brainstorming ideas or templates • Grammar or formatting assistance	• Line manager awareness • Human review before use • No confidential or personal data input
Medium Risk	AI use that involves non-sensitive personal information, internal business data, or could influence decisions but does not determine outcomes independently.	• Drafting job advertisements or training materials • Assisting with performance summaries (non-decisive) • Customer communication drafts • Internal data analysis using approved tools	• Manager approval • Use of approved AI systems only • Mandatory human oversight and validation • Compliance with privacy and discrimination laws
High Risk	AI use that may affect legal rights, employment outcomes, safety, compliance, or involves sensitive personal information or automated decision-making.	• Recruitment screening or selection decisions • Performance management or disciplinary recommendations • Safety-critical diagnostics or risk assessments • Automated customer decisions impacting rights or entitlements	• Executive, Legal, IT and Compliance approval • Formal risk and privacy impact assessment (PIA) • Human-in-the-loop decision-making required • Ongoing monitoring, audit, and documentation

Where an AI use case does not clearly fall within one category, it must be treated as **High Risk** until reviewed and approved.

The Group is committed to responsible AI governance and will:

- Maintain internal processes to assess ethical, legal, and operational risks associated with AI;
- Apply human-in-the-loop controls for high-impact or high-risk AI use cases;
- Monitor AI systems for bias, accuracy, and unintended consequences;
- Maintain feedback and reporting mechanisms for concerns or improvement opportunities.

10. Breaches

Breaches of this policy may result in disciplinary action up to and including termination of employment and may also expose the individual and the Group to legal or regulatory consequences.

Refer to the Disciplinary Policy for further information.

11. Policy Review

This policy will be reviewed at least every 12 months, or earlier if required due to legislative change, regulatory guidance, or business needs.



12. Policy Status

This Policy does not form part of any employee's contract of employment. It is a lawful and reasonable direction of the Company with which compliance is required. Any statement in this Policy about what the Company will or will not do does not create a legally binding obligation on the Company.

This Policy may be amended from time to time to reflect changes in legislation, regulatory requirements or organisational needs.