RESPONSIBLE ARTIFICIAL INTELLIGENCE POLICY

OF

APOLLO PIPES LIMITED

Version	Revision Date	Approved by	Date of Approval
1st Version		Board of Directors	05.11.2026

1. Introduction

Apollo Pipes Ltd will use and build Artificial Intelligence (AI) only in ways that are secure, lawful, fair, transparent, accountable, human-centric and environmentally responsible. AI can support many of our activities, including data analysis and operational decision-making. These benefits come with risks to personal data, confidential information, business continuity, stakeholders and the environment. This policy sets the boundaries for how AI is selected, developed, procured, deployed and operated across Apollo Pipes Ltd. It forms part of its information security, data protection and risk management framework.

2. Objectives

This policy enables AI-driven innovation while preventing misuse, unintended harm and unmanaged risk.

Specifically, it aims to:

- Protect personal, sensitive and confidential information processed by AI systems.
- Secure AI systems, models and data against cyber threats and misuse.
- Ensure AI outcomes are fair, explainable and subject to meaningful human oversight.
- Assign clear ownership and accountability for every AI system in use.
- Keep AI use within applicable laws, regulations and contractual obligations.
- Reduce the environmental footprint of AI across its lifecycle.

3. Scope and Applicability

This policy applies to everyone who uses or works on AI for or on behalf of Apollo Pipes Ltd, and to every AI system it owns, licenses or relies on.

People covered: all employees (permanent, contractual and temporary), interns, vendors, service providers, third-party consultants, associates and business partners.

Systems covered: AI and machine-learning models, generative AI tools, datasets and data lakes used for training or inference, AI platforms and applications, automated decision-support systems, and AI features embedded in other software. This includes systems that are developed in-house, procured, licensed, subscribed to as a service, or operated by service providers on Apollo Pipes Ltd's behalf.

4. Definitions

Term	Meaning in this policy
AI system	Software that generates predictions, recommendations, content or decisions from data, with some degree of autonomy.
Generative AI	AI that produces new text, images, code, audio or video in response to prompts.
AI system owner	The business or process owner accountable for an AI system's purpose, use and outcomes.
High-risk AI use	A use that could significantly affect people's rights, safety, employment, finances, critical infrastructure or legal compliance.
Human oversight	The ability of designated personnel to review, intervene in, override or stop an AI output or system.
Personal data	Any data about an identified or identifiable individual, as defined under the Digital Personal Data Protection Act, 2023 and other applicable laws.
AI incident	Any event in which an AI system causes or nearly causes harm, a data breach, a security compromise, a biased outcome or a regulatory breach.

5. Policy Commitments and Guiding Principles

Apollo Pipes Ltd commits to the following nine principles for every AI system within scope:

1. Privacy and data protection. Personal, sensitive and confidential data used by AI is collected, processed, stored, shared, retained and deleted only as permitted by law, including the Digital Personal Data Protection Act, 2023, and internal data classification rules. Data minimization and anonymization are applied wherever feasible.
2. Security by design. AI systems, models, datasets and infrastructure are protected through access control, encryption, secure development, vulnerability testing, logging, monitoring and incident response. Controls specifically address AI threats such as prompt injection, data poisoning, model theft and harmful outputs.
3. Fairness and non-discrimination. AI is designed and used inclusively. Bias is identified and reduced through representative data, testing before and after deployment, and corrective action.
4. Human oversight. AI must not make irreversible, high-risk or critical decisions without review and approval by a designated person. That person can intervene in, override, suspend or escalate any AI output.
5. Transparency and explainability. People are told when they are interacting with AI or are materially affected by an AI-driven decision. AI outputs used in decisions are explainable to the users and decision-makers who rely on them.
6. Accountability. Every AI system has a named owner. Responsibility for decisions and outcomes influenced by AI stays with that owner or designated authorized personnel, never with the tool.
7. Defined purpose and boundaries. Each AI system has a documented purpose, approved use cases, permitted users, data inputs, output limits and escalation route. It must not be used beyond these boundaries.
8. Environmental responsibility. Apollo Pipes Ltd shall consider and seek to minimize the environmental impact and ecological footprint of its AI tools, supporting infrastructure and technology providers through energy-efficient technologies, responsible use of computing

resources, sustainable data Centre operations and promotion of sustainability throughout the AI lifecycle.

9. No manipulation or exploitation. Apollo Pipes Ltd shall not knowingly develop, procure, deploy or use AI systems that engage in manipulative or deceptive behavior, exploit the vulnerabilities of individuals or groups, or carry out real-time remote biometric identification, except where expressly permitted under applicable law and approved through appropriate governance review.

6. Governance, Roles and Responsibilities

The Board, through its Risk Management Committee, oversees this policy, and every AI system has a named owner accountable for its day-to-day use.

Role	Key responsibilities
Board / Risk Management Committee	Approves this policy; approves high-risk AI uses and exceptions; reviews material AI risks and incidents at least annually.
CEO / Executive Management	Sponsors responsible AI; ensures resources for implementation; ensures an up-to-date inventory of AI systems is maintained.
Data Protection Officer	Ensures lawful data processing; conducts or approves data protection impact assessments.
AI system owner	Documents purpose and boundaries; ensures human oversight; monitors performance and bias; reports incidents.
Developers and data scientists	Build and test AI securely and fairly; maintain model documentation.
Procurement	Applies AI due diligence and contract clauses to vendors.
All users	Use only approved AI tools, within approved purposes, and report concerns promptly.

7. Risk Classification and Approval

Risk tier	Examples	Approval required
Prohibited	See section 8.2	Not permitted
High	Hiring or performance decisions, control of grid or plant operations, credit or pricing decisions affecting individuals, processing sensitive personal data	Board / Risk Management Committee, after security review and data protection impact assessment
Medium	Energy generation forecasting, predictive maintenance, customer-facing chatbots	Data Protection Officer review; business head sign-off
Low	Drafting internal documents, summarising public information, code assistance on non-sensitive code	Use of an approved tool from the AI tool register

Approval flow: Use case proposed □ Registered in AI inventory □ Risk assessment □ Approval per risk tier (Low: approved tool; Medium: DPO review and business head sign-off; High: Board / Risk Management Committee approval) □ Deploy and monitor.

High-risk systems are re-assessed at least annually and whenever their purpose, data or model changes significantly.

8. Acceptable and Prohibited Use

8.1. Acceptable use of generative AI by employees

Employees may use generative AI tools listed on the approved AI tool register, provided they:

- Do not enter confidential, personal, financial, customer or proprietary data into public or unapproved AI tools.
- Review and verify all AI-generated content for accuracy before relying on or sharing it.
- Take personal responsibility for any work product that includes AI output.
- Disclose AI assistance where it materially shaped a deliverable shared externally.
- Respect intellectual property rights and do not use AI to reproduce copyrighted material without permission.

8.2 Prohibited uses

Apollo Pipes Ltd will not knowingly develop, procure, deploy or use AI to:

- Manipulate or deceive people, or exploit the vulnerabilities of individuals or groups.
- Conduct social scoring of employees, customers or communities.
- Carry out unauthorized biometric surveillance, including real-time remote biometric identification, unless
- Expressly permitted by law and approved by the Board / Risk Management Committee.
- Make fully automated decisions on hiring, dismissal, discipline or compensation without human review.
- Generate misleading content, deepfakes or impersonations of real people.
- Bypass security controls, attack systems or create malicious code.

9. Third-Party and Vendor AI

- Vendors that supply or use AI for Apollo Pipes Ltd must meet the same standards as internal teams.
- Procurement and the AI system owner will:
- Assess the vendor's AI security, data handling, bias testing and transparency practices before contracting.
- Include contract clauses on data ownership, confidentiality, restrictions on using Apollo Pipes Ltd data to
- train vendor models, audit rights, incident notification timelines and compliance with this policy.
- Confirm where Apollo Pipes Ltd data is stored and processed, including any cross-border transfers.
- Review high-risk vendors at least annually.

10. Training, Incidents, Compliance and Review

- Training and awareness- Developers, AI system owners and approvers receive role-specific training.
- Incident reporting- Anyone who suspects an AI incident, such as a data leak, harmful or biased output, or security compromise, must report it immediately to the AI system owner. Incidents are handled under Apollo Pipes Ltd's cyber security incident response process, and personal data breaches are notified as required by law.
- Monitoring and audit- Internal Audit periodically reviews compliance with this policy.

- Exceptions- Any deviation from this policy needs prior written approval from the Board / Risk Management Committee, with documented reasons and compensating controls.
- Violations- Breaches of this policy may lead to disciplinary action up to termination of employment or contract, in addition to any legal consequences.
- Policy review- This policy and the effectiveness of its implementation are reviewed at least annually, or sooner when laws, technology or business needs change significantly.
- Governance- Apollo Pipes Ltd shall establish appropriate governance structures, oversight mechanisms and accountability frameworks to support compliance with this policy. The Board is the highest decision-making authority responsible for overseeing the implementation of this policy.