

OneSource Responsible Artificial Intelligence Policy

Purpose and Scope

OneSource Specialty Pharma Limited (“OneSource”, or “the Company”) is committed to the responsible, ethical, secure, and transparent use and development of Artificial Intelligence (AI). This policy sets out the principles and expectations that govern AI technologies used, developed, integrated, or deployed by OneSource during its business activities. It applies to all employees, contractors, consultants, temporary personnel, and third parties acting on behalf of OneSource. The policy covers all forms of AI technologies, including generative AI, machine learning systems, AI-enabled automation, image and content generation tools, AI-assisted coding, and AI functionality embedded in business applications or enterprise systems.

Data Privacy in the Use and Development of AI

OneSource is committed to protecting personal data and sensitive information throughout the full lifecycle of AI, from design and development through deployment, use, and retirement. AI systems must be used in accordance with applicable data protection and privacy laws, including India’s Digital Personal Data Protection Act, 2023, the GDPR where applicable, and other relevant laws in the jurisdictions in which OneSource operates.

Personal data and special-category or sensitive information must only be processed through AI systems where there are a valid legal basis and appropriate safeguards are in place. These safeguards may include contractual protection, data processing agreements, privacy assessments, restricted access, and data minimisation measures. Confidential, regulated, health-related, clinical, patient, or otherwise sensitive information must not be entered into AI tools unless such use is authorised, lawful, and protected by suitable controls.

Cybersecurity and Protection of AI Systems

OneSource will implement and maintain appropriate security measures to protect AI systems and related environments from misuse, unauthorised access, compromise, and cyber threats. AI tools must be subject to appropriate review, approval, and security assessment before they are introduced for business use.

Security controls may include strong authentication, encryption, secure coding practices, access management, vulnerability monitoring, vendor due diligence, and safeguards designed to reduce the risk of harmful, inappropriate, or malicious outputs. Any suspected AI-related security incident, vulnerability, misuse, policy breach, or other concern must be promptly reported through established channels and subject to appropriate management oversight and review. Where necessary, suitable corrective and preventive actions shall be taken to mitigate risks, address identified issues, and support the secure, ethical, and responsible use of AI systems.

Fairness and Prevention of Bias

OneSource is committed to promoting fairness, objectivity, and non-discrimination in the use and development of AI. Reasonable steps must be taken to identify, assess, and reduce the risk of bias in AI systems, training data, prompts, and outputs.

AI must not be used to generate, support, or distribute content or outcomes that are discriminatory, defamatory, deceptive, or otherwise harmful. In situations where AI outputs may affect individuals, business decisions, quality outcomes, compliance obligations, or safety-related matters, OneSource encourages the use of representative data and the periodic review of AI outputs to help identify and address unfair or inequitable results.

Human Oversight and the Ability to Intervene

OneSource requires meaningful human oversight over AI-assisted activities, particularly where outputs may influence important operational, legal, regulatory, quality, safety, or customer-related matters. AI-generated work,

recommendations, analysis, or content must be reviewed, checked, and validated by suitably qualified personnel before being relied upon or used.

AI systems must not be allowed to make final, irreversible, or high-impact decisions without human review and the ability to intervene, override, or escalate concerns. This includes decisions affecting safety, regulatory compliance, contractual commitments, or the rights and interests of individuals. The use of AI does not reduce personal responsibility, and employees are expected to apply judgment when using AI-supported outputs.

Transparency and Explainability

OneSource will promote transparency in relation to the use of AI across its operations. Where appropriate, employees must disclose the use of AI in preparing work products, communications, analysis, or decision-support materials. AI-assisted outputs should be identified or labelled where required by law, internal policy, contractual obligation, or business need.

Where individuals interact with an AI-enabled system, OneSource will seek to ensure that such interaction is not misleading and that it is clear, where appropriate, that the interaction involves AI rather than only a human. To the extent practicable and relevant, OneSource will also support the ability to explain AI-generated outputs or recommendations in a way that is understandable to the intended audience.

Accountability for AI Outcomes

Responsibility for decisions, actions, and outcomes supported by AI remains with OneSource and its personnel, not with the technology itself. Clear ownership must be assigned for oversight of AI use, risk management, compliance review, and issue resolution.

OneSource will maintain governance arrangements to review AI-related risks, assess appropriate use cases, and investigate incidents, errors, or adverse effects arising from AI use. Employees and other authorised users remain accountable for the quality, accuracy, legality, and appropriateness of any AI-assisted work they create, rely upon, communicate, or implement.

Clear Limits on the Use of AI

OneSource will define and enforce clear boundaries regarding the approved use, capabilities, and limitations of AI systems. This includes setting expectations around authorised use cases, permitted data inputs, access controls, review requirements, and escalation pathways for higher risk uses.

The use of unapproved AI tools, personal AI accounts for company business, or unauthorised integration of AI into internal systems is prohibited. Any AI capability introduced into systems that support regulated, quality-relevant, or controlled business processes must be subject to appropriate review, validation, and approval before use.

Environmental Considerations

OneSource recognises that AI technologies may have environmental impacts, including energy consumption, water use, and carbon emissions associated with computing infrastructure and model operation. While balancing business needs and innovation, OneSource aims to remain mindful of these impacts when selecting, developing, and using AI solutions.

Where feasible, OneSource will encourage efficient use of computing resources, optimisation methods that reduce unnecessary processing demands, and consideration of environmentally responsible practices by third-party AI providers and hosting partners.

Compliance with Applicable Laws and Regulations

OneSource will use and deploy AI in a manner consistent with all legal and regulatory requirements relevant to its operations. Depending on the nature of the activity, this may include obligations relating to privacy, information security, quality, healthcare, life sciences, records, and electronic systems.

Where applicable, AI processing involving personal data must comply with the Digital Personal Data Protection Act, 2023, as well as the GDPR and other relevant privacy laws in jurisdictions where OneSource operates. Where AI is used in regulated or quality-relevant activities, it must align with applicable standards such as GMP, GCP, GVP, FDA 21 CFR Part 11, EU Annex 11, ICH Q10, GAMP 5, and other relevant frameworks. AI capabilities introduced into regulated systems must undergo appropriate validation, including Computer System Validation, before they are used operationally.

Prohibited AI Practices

OneSource prohibits the use or deployment of AI for unlawful, unethical, deceptive, or harmful purposes. This includes AI systems or uses that manipulate or improperly influence individuals, exploit vulnerabilities relating to age, disability, health status, or socioeconomic condition, or enable social scoring of individuals.

OneSource also prohibits the use of AI for unauthorised biometric identification, tracking, or surveillance, as well as for generating discriminatory, defamatory, false, or misleading content. AI must not be used to impersonate individuals, facilitate fraud or misconduct, or bypass established security, access, compliance, or governance controls.

EU AI Act

The European Union Artificial Intelligence Act (Regulation (EU) 2024/1689) applies to certain providers, deployers, importers, distributors, and other parties whose AI systems are placed on the market, put into service, or whose outputs are used within the European Union in a way that brings them within scope.

Based on OneSource's current business profile, operations, and known AI use cases, the organisation may not presently fall within the direct scope of the EU AI Act. However, this position will remain under review. If future changes in business activities, customer engagements, product offerings, market presence, or AI deployment bring OneSource within the scope of the EU AI Act or similar regulation, OneSource will assess its AI systems against applicable requirements and update its governance, controls, documentation, and disclosures accordingly. OneSource will continue to monitor evolving AI laws and standards to support ongoing compliance across relevant jurisdictions.

Governance, Review, and Approval

This policy will be administered through OneSource's governance framework for risk, compliance, quality, and information security. Relevant oversight functions may include the review of AI-related risks, approval of higher-risk use cases, monitoring of compliance obligations, and management of incidents, exceptions, or remediation actions.

The policy will be supported through appropriate training, awareness initiatives, and internal controls. It will be reviewed periodically, and at least annually, or sooner where required due to changes in law, technology, business operations, or AI-related events.

Version Control Sheet

Version Number	Date of Board Meeting	Remarks
V1	Approved and adopted in the Board Meeting held on July 24, 2026	Adopted in line with requirements of ESG parameters