STRIDES PHARMA SCIENCE LIMITED

Responsible Artificial Intelligence Policy

Approved by the Board on August 27, 2026

Strides

1. Purpose & Scope

Strides Pharma Science Limited, along with its subsidiaries (together referred to as "Strides", "We", "The Company") is committed to the responsible, ethical, secure, and transparent use and development of Artificial Intelligence (AI). This policy sets out the principles governing all AI systems and models we use or deploy whether developed internally or provided by third parties across our operations. It applies to all employees, contractors, and third-party providers acting on our behalf, and covers all AI technologies including generative AI, AI-powered automation, image generation, AI-assisted coding, and AI-integrated business applications.

1.1 Definitions

For the purpose of this Policy, an "AI System" means a machine-based system that generates outputs such as predictions, content, recommendations, classifications, or decisions that may influence physical or digital environments.

"High-Impact AI" means an AI system whose use or output may materially affect patient safety, product quality, clinical or pharmacovigilance obligations, regulatory compliance, employment, privacy, legal rights, cybersecurity, financial reporting, or other significant stakeholder interests.

1.2 Human-Centred and Beneficial Use of AI

Strides use AI to augment human capabilities, improve productivity, support scientific and operational insights, and contribute to better healthcare outcomes. AI shall support, and not improperly replace, human judgment, professional expertise, dignity, autonomy, or accountability. Appropriate consideration shall be given to patient welfare, employee interests, customer expectations, and broader societal impacts.

2. Respecting Data Privacy in the Use and/or Development of AI

We safeguard personal data throughout the lifecycle of AI development and deployment. We design, develop, and operate AI systems in compliance with applicable data protection laws, including India's Digital Personal Data Protection (DPDP) Act, 2023, the GDPR, and equivalent laws in the jurisdictions in which we operate. Personal and special-category data including health, clinical, and patient information is protected through controls such as Data Processing Agreements and Data Protection Impact Assessments and is not entered into AI tools without a lawful basis for processing.

3. Protecting the Cybersecurity of Systems in the Use and/or Development of AI

We apply robust security measures to prevent cyberattacks across our AI systems. These include the use of approved and validated tools, multi-factor authentication, encryption, secure coding and access controls, vendor security assessments, and mechanisms to prevent harmful or inappropriate content. Suspected security incidents involving AI are reported and managed through our incident management and response process.

Suspected AI-related incidents, including data leakage, cybersecurity compromise, unauthorised use, materially inaccurate or harmful output, operation outside approved parameters, or validation failure, shall be reported promptly. Strides shall investigate such incidents, contain resulting risks, implement corrective and preventive actions, and make any legally or contractually required notifications.

4. Avoiding Potential Bias in the Use and/or Development of AI

We are committed to fair and non-discriminatory AI behaviour. We identify and mitigate bias in the AI systems we use, and we prohibit the use of AI to generate discriminatory, defamatory, or misleading content. Recognising the patient-safety implications of bias in a pharmaceutical context, we promote the use of representative data and the periodic review of AI outputs for fairness and equity.

5. Keeping Humans "in the Loop" for Critical Decisions and Allowing Human Intervention

We maintain human oversight (human-in-the-loop) over AI-influenced decisions. All AI-generated outputs are reviewed, verified, and validated by a qualified person before use. AI systems may not make irreversible or high-stakes decisions including those affecting patient safety, regulatory compliance, or client obligations without documented human oversight and the authority and ability to intervene, override, or escalate.

6. Ensuring Transparency of AI Systems and Explainability of AI-Generated Results/Decisions

We provide clear disclosure of AI use, including its capabilities, limitations, and risks. Employees disclose AI usage where required, and AI-assisted work is appropriately labelled. Where AI interacts with individuals, it will be clear that they are interacting with an AI system rather than a human, and we provide an understandable rationale for AI outputs appropriate to stakeholders' needs.

7. Clear Accountability for Outcomes Produced by AI Models/Tools

Accountability for AI outcomes rests with named roles. Our AI Governance Committee, supported by the IT Security team, the Quality/Compliance function, and Function Heads, is responsible for oversight, risk decisions, and compliance. We maintain a process for investigating and addressing errors or harm arising from AI use through our incident management process, and employees remain personally accountable for the accuracy and quality of AI-assisted work.

8. Usage guidelines for Employee

8.1. As part of Strides' commitment to secure, compliant, and responsible AI adoption, Microsoft Copilot (as approved and made available by Strides) shall be the primary AI tool for business use across the organisation. Employees are expected to use only AI tools and services that have been reviewed and authorised by the Company and in line with the internal guidelines launched by the Company in this regard.

Employees shall not enter personal data, patient information, confidential information, trade secrets, regulated records, proprietary source code, formulations, manufacturing information, unpublished scientific or regulatory information, or third-party protected material into an AI system unless the use has been specifically authorised and is supported by appropriate legal, privacy, security, contractual, and technical controls.

Any request to procure, subscribe to, or use a paid AI tool, platform, model, or AI-enabled software outside the approved corporate AI portfolio must be submitted for review and prior approval by the AI Governance Committee and relevant stakeholders, including IT Security, Quality/Compliance, and Finance and Procurement, as applicable. The review shall consider the following and in line with the internal guidelines launched by the Company in this regard:

- Business need and expected benefits;
- Information security and cybersecurity risks;
- Data privacy and regulatory requirements;
- Cost and licensing considerations;
- Intellectual property and contractual obligations;
- Vendor and third-party risks;
- GxP and validation requirements, where applicable

8.2. Employee Responsibilities

Employees using AI systems shall:

- Use AI only for authorised business purposes and within the approved scope of use;
- Verify the accuracy, completeness, appropriateness, and reliability of AI-generated outputs before relying on or sharing them;
- Protect personal, confidential, proprietary, regulated, and third-party information;
- Avoid relying on AI as the sole basis for high-impact or irreversible decisions;
- Comply with applicable requirements relating to intellectual property, records management, data integrity, GxP, and information security;
- Disclose AI use where required under this Policy or applicable internal procedures. And;
- Promptly report suspected incidents, harmful outputs, data leakage, bias, security concerns, or unauthorised use

8.3. **Non-Compliance:** Use of unapproved AI tools, services, or personal AI accounts for business purposes is prohibited. The use of unapproved AI tools or bypassing the required review and approval process constitutes a policy violation and may result in access restrictions and disciplinary action in accordance with Company policies/ guidelines.

9. Clear Boundaries for What the AI Can and Cannot Do

We define the authorised scope, capabilities, and limitations of our AI systems to prevent misuse, mission creep, or unintended application. This is enforced through allowed-use rules, approved-tool lists, guardrails, capability restrictions, and control points for escalation. The use of unapproved tools or personal AI accounts for work, and the

integration of AI into systems without formal Computer System Validation (CSV), is prohibited.

10. Requiring (Own/Third-Party) AI Data Centers/Models to Have a Low Ecological Footprint

We aspire to be mindful of the ecological footprint of the AI systems we use and deploy, including those provided by third parties. We aim to support approaches that help better understand and, where feasible, reduce the energy use, water use, and carbon intensity associated with AI workloads. This includes encouraging optimisation techniques that can lessen computational demand and energy waste, and giving consideration, where appropriate, to the environmental practices of third-party providers.

11. Regulatory Compliance & Prohibited AI Practices

11.1. Regulatory Framework Applicable to Strides

As a generic pharmaceutical company operating primarily under Indian and other applicable jurisdictions, Strides uses, and deploys AI systems in compliance with the laws and regulatory frameworks applicable to our operations, including:

- **Digital Personal Data Protection (DPDP) Act, 2023:** All AI deployments involving personal or patient data comply with the DPDP Act and, where applicable, the GDPR and equivalent data protection laws in the jurisdictions in which we operate.

- **GxP and Validation Standards**: AI used in regulated activities is governed by Good Manufacturing, Clinical, and Pharmacovigilance Practices (GMP, GCP, GVP), FDA 21 CFR Part 11, EU Annex 11, ICH Q10, and GAMP 5 guidelines. Any AI integrated into regulated systems undergoes a formal Computer System Validation (CSV) process before deployment.

11.2. Prohibited AI Practices

Consistent with global responsible-AI standards, Strides does not use or deploy AI systems that engage in manipulative or deceptive behaviour, that exploit vulnerabilities relating to age, disability, or socioeconomic circumstance, that perform social scoring of individuals, or that conduct unauthorised or real-time remote biometric identification and surveillance. We further prohibit the use of AI to generate misleading, defamatory, or discriminatory content, to impersonate individuals, to facilitate fraud, or to circumvent security and access controls.

12. Governance, Review & Endorsement

This policy is governed by an internal AI Governance Committee. The policy shall be supported by employee training and awareness programmes and is subject to ongoing monitoring, internal audit, and formal review on a periodic basis or following any significant change in technology, regulation, or AI-related incident.

The governance framework for overseeing our policy is firmly rooted in the leadership and strategic direction provided by the highest governing body within our organisation under the advisement of the board-level Risk Management and Sustainability Committee (RM&SC). This committee operates with a clear mandate to ensure that all cyber security initiatives, including AI governance align with our core values and strategic objectives, while meeting regulatory and stakeholder expectations.

13. Review and Amendments

Strides reserves its right to amend or modify this policy, in whole or in part, at any time without assigning any reason, provided such changes are approved/ ratified by the Board.

Group General Counsel, Quality Head, HR Head and IT Head of the Company are severally authorized to amend the policy to give effect to any changes or amendments as may be required to advance internal practices or as may be required to align with any applicable laws, rules and regulations. The Amended policy shall thereafter be placed before the Board for noting and ratification.

The Board shall have the power to amend any of the provisions of this Policy, substitute any of the provisions with new provision or replace this Policy entirely with a new Policy.

This policy serves as a commitment statement and should be read in conjunction with Strides' internal SoPs and guidance notes, applicable to employees in general and to specific departments, which provide the operational framework and procedures governing the use of AI.

*****