



Responsible AI

2025-26



Responsible AI and digital ethics

Artificial intelligence is increasingly central to how Coforge creates value for clients and manages internal operations. As we embed AI into business processes and decision-making, the need for responsible AI and robust digital ethics is critical. We recognise that ethical considerations are integral to the design, deployment, and governance of AI systems, and our AI Governance Framework is designed to ensure that digital solutions are not only powerful but principled. Our approach embeds ethical safeguards, transparency, and human oversight across the AI lifecycle, enabling us to create sustainable value while safeguarding stakeholder interests.

Management approach

AI is a key enabler for how Coforge manages risk, drives efficiency, and delivers on its strategic and sustainability commitments. We believe that the responsible use of AI is inseparable from long-term business integrity.

Coforge has established an AI Governance Framework that defines the boundaries, responsibilities, and processes for managing AI systems responsibly. The framework:

- Applies across all departments, functions, and teams that design, develop, deploy, or use and monitor AI.
- Ensures consistency in governance whether AI is used internally (e.g., HR analytics) or externally (e.g., client delivery).
- Covers every stage of the AI lifecycle: Plan & Design, Data Governance, Develop & Train, Verify & Validate, Deploy & Integrate, Operate & Monitor, and Retire or Replace.
- Aligns with international standards and regulations, including ISO/IEC 42001:2023, the EU AI Act, and the NIST AI Risk Management Framework (AI RMF).

Our Responsible AI Policy establishes the ethical principles that guide this work, including fairness and inclusiveness, transparency, privacy, safety and reliability, human oversight, regulatory compliance, and security. These principles apply equally to AI systems used internally and to AI solutions developed for and deployed on behalf of clients.

- Clearly defined boundaries prohibit the use of AI for manipulative behaviour, exploitation of vulnerabilities, unauthorized surveillance, or other high-risk applications that may negatively impact individuals or society.
- The policy promotes transparency in AI-enabled decision-making, ensuring outputs are interpretable where relevant and subject to appropriate human validation.

Coforge on AI ethics commitment

Coforge is committed to the responsible, ethical, and secure use of AI across the organisation. We will ensure transparency in AI-driven decisions, uphold fairness by actively identifying and mitigating bias, and protect data privacy through robust governance and compliance with global standards. Our approach prioritises human oversight, accountability, and continuous risk assessment, ensuring AI solutions align with our business values, regulatory obligations, and societal expectations. We will invest in awareness, controls, and auditing mechanisms to ensure AI is deployed to augment human capability while maintaining trust, integrity, and resilience.



Governance structure

Governance of responsible AI is an executive-level responsibility. Chief Information Officer (CIO) is the executive authority responsible for approving AI-related policies and ensuring that AI governance aligns with the organisation's IT strategy, providing enterprise-level accountability for safe and effective AI adoption.

Coforge has established the following governance structure for AI:

Role	Accountability
CIO	Executive authority; approves AI-related policies; ensures alignment with IT strategy and enterprise-level accountability for AI governance.
AI Governance Council	Provides enterprise-level oversight; approves the AI Governance Framework, policies, and major updates; oversees overall governance effectiveness.
AI Governance Working Group (CIO Function, CDO Function & HBUs)	Cross-functional expert group overseeing enterprise-wide AI governance, risk management, and alignment with strategic AI objectives. Manages AI Inventory, risk tiering, impact assessments, approvals and exceptions, regulatory alignment, and role-based training and awareness. Reports on overall AI governance posture to the AI Governance Council.
IBU / HBU / Function Heads	Business leaders with departmental ownership of AI systems, including risk oversight, inventory consolidation, and approval of key lifecycle decisions. Ensure AI adoption aligns with business goals while maintaining compliance, accountability, and operational integrity.
AI System Team (Owner, Development, Validation)	Designs, develops, operates, and maintains AI systems across their lifecycle. The System Owner is accountable for system purpose, compliance, monitoring, and risk management. The Development Team ensures data quality, documentation, testing, and compliance. The Validation Team independently reviews systems for fairness, safety, transparency, regulatory adherence, and readiness for deployment.
Support Functions	Provide governance, security, privacy, procurement, licensing, HR, capability development, and operational support. Ensure AI requirements are integrated into organisational processes and that AI systems comply with applicable policies, regulatory obligations, and technical safeguards.
End Users	Interact directly with AI systems and are responsible for safe, compliant usage in accordance with AI usage policies. Serve as the first line of defence in identifying anomalies, escalating risks, and reporting incidents.

Policies, risk management, and the AI lifecycle

Coforge's AI Governance Framework is operationalised through a comprehensive set of policies and supporting documents that cover the full AI lifecycle from initial system classification to decommissioning. Key policies include:

- AI Acceptable Usage Policy
- Responsible AI Policy
- AI Incident Management Policy
- AI Risk Management Policy
- AI Lifecycle Policy

All AI systems are assigned to a risk tier of High, Medium, or Low. The risk tier determines applicable governance controls, the depth of independent validation required, and the intensity of operational monitoring. High-risk AI systems, such as those used in sensitive domains or involving significant impact on individuals and society, are subject to independent validation by the Validation Team for fairness, safety, transparency, robustness, and regulatory adherence prior to deployment. Risk management is aligned with the NIST AI RMF. All identified AI risks are maintained in an AI Risk Register, with associated controls tracked through the AI Risk Control Mapping. The AI Governance Working Group reviews this risk information on an ongoing basis.

AI systems are subject to fairness and bias assessments, particularly for high-risk use cases, to ensure equitable and non-discriminatory outcomes. AI-generated outputs are required to be reviewed and validated by human users and are not to be misrepresented as fully human-generated, ensuring transparency in AI-assisted decision-making and content creation.

Changes to AI systems are managed through a formal change management process that includes approval workflows for model updates or retraining, documentation of rollback and failover plans, and full audit trails. AI incidents are managed under the AI Incident Management Policy, which covers identification, assessment, escalation, mitigation, and post-incident review. Where applicable, AI-supported outcomes may be subject to human review and reassessment to ensure accountability, fairness, and appropriate resolution of concerns.

Data privacy and security in AI systems

The responsible handling of data in AI systems is a foundational requirement. Coforge's AI governance policies are designed to comply with India's Digital Personal Data Protection (DPDP) Act and other applicable data protection and privacy regulations.

Privacy-by-design and security-by-design principles are embedded throughout the AI lifecycle. The AI Access Management Policy ensures that only authorised personnel can access AI systems, data, and models.

To ensure secure and responsible use of AI systems, Coforge:

- Monitors AI tool usage across corporate systems and networks.
- Reviews data shared with AI tools to verify adherence to data protection and confidentiality requirements.
- Blocks unapproved AI sites or applications to prevent unauthorised usage.
- Employees are explicitly prohibited from uploading confidential, personal, or proprietary data, including customer information, internal documents, and source code into external AI tools.

All monitoring activities are conducted in compliance with applicable privacy regulations, data protection laws, and Coforge's Information Security Policy. The Generative AI Consent Form governs the use of personal and sensitive data in generative AI contexts.

Third-party and vendor AI

Coforge's AI Procurement and Vendor Management Policy establishes a systematic approach to acquiring and managing third-party AI solutions. All AI vendors are subject to due diligence before onboarding, with assessments covering ethical alignment, regulatory compliance, security and privacy controls, and accountability throughout the relationship lifecycle. Vendor due diligence is integrated into the AI Lifecycle Tracker to ensure consistent application of controls across the AI portfolio.

Coforge also assesses vendors on their adherence to responsible AI practices, including ethical use, transparency, and alignment with sustainability considerations where relevant.

Training and Awareness

Coforge promotes responsible AI adoption through a structured training and awareness programme for employees and contractors involved in the use, development, or oversight of AI systems. The programme includes onboarding and periodic refresher training on responsible AI principles, governance requirements, acceptable use practices, and incident reporting mechanisms. Awareness is reinforced through regular communications and engagement initiatives, while the AI Governance Council oversees capability building to support consistent implementation of AI governance practices across the organisation. For high-risk AI applications, including those involving sensitive personal data or sector-specific use cases such as healthcare, finance, and law enforcement, additional role- and project-specific training is provided to address relevant risks, regulatory obligations, and ethical considerations.

Training name	Mode	Brief on training	Number of attendees
Enterprise AI Literacy – Foundation	Virtual (enterprise learning platforms)	Foundational AI awareness programmes aimed at building baseline AI literacy across technical and non-technical workforce	19,000+ trained
Intermediate AI Capability	Virtual + hands-on practitioner-led sessions	Practitioner-led, applied AI learning focused on building deployment-ready capabilities within delivery teams	15,000+ trained
Advanced AI Capability	Virtual (certification-based)	Role-based AI agent design and deployment capability, enabling advanced AI engineering skills	15,000+ trained
Leadership Enablement	Virtual sessions for leadership enablement	Business-led AI sessions focused on enterprise use cases and Coforge-built AI solutions for leadership alignment	3,000+

240K+ hours

Total AI learning hours delivered

~90%+

Workforce AI enablement

These programmes include guidance on responsible AI usage, ethical risks, and appropriate handling of AI-generated outputs, reinforcing accountability across all levels of the organisation.



Registered Office

Coforge Limited

Plot No. 13, Udyog Vihar, Phase-IV,
Sector-18, Palam Road,
Gurugram - 122015, Haryana, India

Tel: 0124-4627837

Corporate Office

Coforge Limited

SEZ Developer Unit,
Plot No TZ 2 & 2A, Sector Tech
Zone, Greater Noida, Gautam
Buddha Nagar, UP-201308.

Tel: 0120-4592300

Website: www.coforge.com | CIN: L72100HR1992PLC128382