STATEMENT ON RESPONSIBLE AI AT ACS:
PRINCIPLES AND PRACTICES

July 2026

Introduction – Commitment to Responsible AI

The ACS Group is advancing the use of AI as a means of improving productivity, safety and sustainability, from design and planning through construction, operation and maintenance of works. We are committed to develop, procure, implement and use AI in a responsible, safe, lawful and ethical manner. This initiative forms part of an "applied AI" approach focused on use cases with a tangible impact: process optimisation, decision-making support, risk reduction and the generation of real-time information to accelerate innovation.

This Responsible AI Statement translates our ACS Group Artificial Intelligence Policy into practical measures aligned with applicable legal and regulatory requirements, safety expectations and broader stakeholder considerations.

Given the evolving nature of AI technologies and regulatory landscapes, the ACS Group applies principles that are designed to be adaptable across jurisdictions and use cases. Our approach is informed by governance frameworks established across the ACS Group of companies, reflecting their respective operational context alongside applicable legislation such as the EU AI Act.

This Statement provides an overview of how Responsible AI is currently governed and applied within the ACS Group, including key principles and practices that guide the use of AI across the Group. It complements existing frameworks across the Group such as the ACS Artificial Intelligence Policy, Code of Conduct, General Compliance Policy, Information Security Policy, Data Protection Policy and the broader compliance framework.

Responsible AI Principles at ACS

Employee Training & Ethical AI Culture: At the ACS Group, training and culture form the foundation of Responsible AI implementation and use. We invest in equipping our workforce with the knowledge and judgement required to use AI safely, legally, ethically, and effectively. Employees gain access to practical guidance and training, including through the ACS University, on AI ethics, security, compliance, and risk awareness - building the baseline capability needed to support Responsible AI controls and governance measures.

From project teams to senior management, our people are developing an understanding of AI capabilities, limitations, and associated risks. Through continuous learning and reinforcement, we embed a culture of accountability, vigilance, and responsible innovation, so that governance measures are not applied in isolation but are actively applied in practice across the Group.

All users of AI systems must adhere to ACS group companies' respective acceptable use policies. In addition, users must not attempt to jailbreak, prompt inject or actively attempt to circumvent protective measures of AI systems or agents.

Accountability: AI is deployed at the ACS Group with a clear expectation of human oversight and accountability. AI systems support, rather than replace, professional judgement, with accountable individuals responsible for their actions and decisions – particularly in safety-critical or high-impact contexts – in line with the ACS Group Code of Conduct and other internal governance policies and frameworks, and consistent with regulatory requirements, for example, human oversight and contestability requirements under the EU AI Act.

Where AI contributes to outcomes that may affect stakeholders, mechanisms and channels are in place to enable those outcomes to be reviewed and, where appropriate, challenged or escalated. This includes enabling concerns to be raised through accessible channels and formal reporting processes, such as the Group's ethical channel or its equivalent channels across the Group.

AI-supported outputs or decisions must be explained and supported, and be able to be challenged, reinforcing accountability and maintaining trust in AI-enabled processes.

Security: At the ACS Group, the security and integrity of the organisation's information together with the information of its personnel and those it works with, is paramount. The collection, access, and storage of personal and other sensitive information, such as client data and intellectual property, are conducted in accordance with applicable laws and are managed and retained under relevant privacy, data protection, and retention policies.

The identification and deployment of AI systems is centrally managed and is limited to approved models and platforms, subject to governance, security, and risk assessment processes. Guardrails are in place to restrict the use of unapproved AI technologies, reducing the risk of inconsistent or uncontrolled use.

Enhanced security risk assessments will apply where proposed AI use impacts decision making involving personal or sensitive data, or where it presents elevated ethical or privacy risks such as biometric identification, with appropriate controls in place where the relevant technology is permitted.

Use is guided by governance principles on appropriate use, responsible roles, and oversight, and is managed in accordance with applicable laws and Group AI Governance, Data Protection/Privacy and Information Security policies.

This approach fosters innovation while supporting the management of risks relating to higher-risk AI technologies under appropriate oversight and accountability.

Transparency: At the ACS Group, AI is currently applied primarily as a support tool (i.e. to aid work activities) with human oversight, rather than operating autonomously. Where AI is used in a substantive or material way, its use is disclosed as appropriate to the context to support transparency.

In situations where AI contributes to outputs or informs decisions, consideration is given to whether users should be made aware of such use, including where interaction with AI systems occurs.

This approach supports informed use, maintains trust, and aligns with evolving regulatory expectations in relevant contexts.

Monitoring: We leverage enterprise-grade AI platforms and tooling and support the responsible deployment, ongoing monitoring, and continuous improvement of AI systems. Deployment is based on approved models and platforms under designated governance and review processes. These enterprise-grade platforms provide capabilities for structured risk identification, performance evaluation, and the detection of issues such as model drift, ungrounded outputs, and emerging security or privacy risks.

AI models in operation are subject to monitoring activities as these capabilities are implemented, with periodic reassessment undertaken where appropriate to support reliability, accuracy, and alignment with intended use. Where required, models may be refined, updated, or replaced to maintain performance and mitigate risks.

By drawing on enterprise technologies and integrated monitoring capabilities, the ACS Group is establishing oversight of AI systems across the Group, reducing the risk of degradation while maintaining alignment with internal policies and evolving regulatory expectations.

Fairness: Fair and unbiased AI outcomes are fundamental. At the ACS Group, consideration is given to potential bias in AI systems and outputs as part of their use. Where relevant, outputs are reviewed to identify unintended or uneven outcomes across different scenarios. The Group also leverages updated AI models with enhanced safety and fairness features to improve reliability and reduce biased outputs.

Where bias or unintended outcomes are identified, use should be refined, controlled, or limited as appropriate. In addition, feedback may be provided to model providers or platform owners, including enterprise vendors, to support ongoing model improvement and risk mitigation.

AI Sustainability Impact: The Group considers, and where relevant, identifies opportunities to better understand and monitor the environmental and social impacts of AI applications, including potential contributions to emissions reductions, resource efficiency, and safety outcomes. This builds on existing enterprise-wide ESG data systems and reporting processes. The current reporting infrastructure provides a foundation to consider the progressive integration of AI-attributable impacts into sustainability reporting over time.