



STATOM HOLDINGS Limited (Statom Group Limited, Statom Group North Ltd, Statom Plant Ltd, Statom Remediation Ltd, Demoforce Group Ltd, FL-Facilities Group Ltd, Slipform Technology Ltd, Spark Tech MEP Ltd, Franki Foundations UK Ltd, Martello Piling Ltd) ("Statom", "the Company")

We are committed to high standards of professional conduct, integrity and accountability. As a leading civil engineering and construction organisation, we recognise that the behaviour and standards of our people are fundamental to building a strong, respectful culture and protecting our reputation as a trusted industry leader.

We expect everyone working for or on behalf of the Company to act with professionalism, respect and responsibility at all times, reflecting our values and supporting a positive working environment. Clear standards of behaviour are essential to ensuring safety, quality and effective collaboration across our projects and teams.

1. Purpose

This policy governs the responsible, lawful and secure use of artificial intelligence tools for Statom business. AI may support productivity and analysis, but it does not transfer accountability away from the person who uses, reviews or approves the output.

2. Scope

It applies to employees, workers, directors, consultants, contractors, suppliers and third parties using AI for Statom business or processing Statom, employee, candidate, client, supplier or project information. It applies to generative AI, machine-learning tools, automated analytics, transcription, meeting assistants, code tools, image tools, plug-ins and integrations.

3. Governance and Approval

- Only approved AI tools may be used for Company business unless IT/Security, Data Protection and the relevant business owner have authorised an exception in writing.
- New tools and high-risk use cases require proportionate security, supplier, data protection, records and contractual review and, where required, a DPIA.
- No AI tool may be connected to Company email, SharePoint, Teams, OneDrive, HR, payroll, finance, project or client systems without IT/Security approval.
- Client or project restrictions override general Company permission.

4. Data Protection and the DUAA 2025

UK GDPR, the Data Protection Act 2018 and all relevant data-protection provisions of the Data (Use and Access) Act 2025 are in force. AI processing must have a lawful basis, be fair, transparent, accurate, secure and limited to what is necessary. Special category and criminal-offence data require the additional statutory conditions and safeguards.

5. Automated Decision-Making

The DUAA 2025 permits solely automated significant decisions in a wider range of circumstances than the previous regime, but statutory safeguards still apply. As a stricter Company control, Statom will not use AI to make a final recruitment, pay, promotion, performance, disciplinary, grievance, capability, redundancy, termination, health and safety or other significant people decision unless HR, Data Protection and Legal/Compliance have approved the specific process. Where applicable, individuals must receive required information, be able to make representations and obtain human intervention.

6. Prohibited Inputs and Uses

- Do not upload personal data, health information, criminal-offence data, payroll/HR records, DSAR material, legal advice, credentials, tenders, pricing, contracts, drawings, designs, method statements, risk assessments or client-confidential information unless the tool and use case are specifically approved.

- Do not use personal AI accounts for Company business where a managed business account is required.
- Do not use AI to impersonate people, fabricate evidence, create deceptive records, bypass approvals or produce unsafe technical/safety-critical decisions.
- Do not use AI outputs as legal, payroll, tax, medical, engineering or regulatory advice without competent human review.

7. Accuracy, Bias and Human Review

AI outputs may be inaccurate, fabricated, biased, incomplete or outdated. Users must verify facts, sources, calculations, technical content and legal or policy references. A responsible human must make and document the final decision where the output materially influences an employee, candidate, client, commercial or safety outcome.

8. Intellectual Property and Confidentiality

Users must not assume AI output is original, non-infringing or owned by Statom. External or client-facing output must be checked for copyright, confidentiality, brand, contractual and professional risk before issue.

9. Meeting Assistants, Recording and Transcription

AI transcription or recording tools require prior approval and appropriate notice. They must not be used in disciplinary, grievance, redundancy, settlement, medical, welfare, investigation, board, legal, confidential client or safety-critical meetings unless expressly authorised. Automated notes are not official records until reviewed and approved.

10. Records, Monitoring and Incidents

Prompts and outputs that materially influence decisions or formal documents may be Company records and must be retained in approved systems. Suspected disclosure, data leakage, hallucinated critical content, unauthorised integration or other AI incident must be reported immediately to IT/Security and, where personal data is involved, the Data Protection Lead.

11. Compliance

Unauthorised or reckless AI use may lead to access restriction, investigation, disciplinary action or contractual consequences. This policy must be read with the IT, Data Protection, Recruitment, Disciplinary, Equality, Confidentiality and Information Security policies.

Approval and Review

This policy will be reviewed at least annually and earlier where legislation, regulatory guidance, case law, Company structure, operational risk or business practice changes materially. Substantive amendments require appropriate Group approval before issue.

AUTHORISED AND APPROVED

SIGNED



Gavin Hunt
Chief Development Officer

Review: Annually
Date: 01/06/2026
Next Review: 01/06/2027

SIGNED



Martina Oyite
Chief People Officer

Review: Annually
Date: 01/06/2026
Next Review: 01/06/2027

*Review: Annually or earlier where legislation, guidance, Company practice or operational requirements change.
This policy is subject to annual review and approval by the Board.*