



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 explains when and how Statom Group may monitor workers, Company systems, workplaces, vehicles and business activity. Monitoring will only be used for a defined and legitimate purpose and must be lawful, fair, transparent, necessary and proportionate. The Company will balance its operational, safety, security and compliance interests against the privacy and data protection rights of workers and other individuals who may be captured.

2. Scope

This policy applies to employees, workers, directors, agency workers, consultants, contractors and any other person using Statom Group systems, devices, premises, vehicles or accounts. It applies in offices, sites, vehicles and remote/home-working environments. Home working does not remove the Company's data protection obligations and normally creates a higher expectation of privacy.

3. Legal and Policy Framework

Monitoring will be managed in accordance with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the Human Rights Act 1998 where relevant, applicable communications and surveillance law, and current ICO employment monitoring guidance. This policy must be read with the Data Protection, IT, AI Usage, Access to Employee Email Accounts, Disciplinary, Whistleblowing and Employee Privacy Notice requirements.

4. Permitted Purposes

- protecting health, safety and security;
- protecting Company, employee, client and supplier property, systems and information;
- preventing, detecting or investigating fraud, theft, cyber incidents, serious misconduct or other unlawful activity;
- meeting legal, regulatory, contractual, client or insurance requirements;
- managing access, attendance, working time and business continuity where proportionate;
- protecting network, email and communications security; and
- supporting quality, service delivery or performance management only where the method is fair, transparent and proportionate.

5. Types of Monitoring

Depending on the purpose and risk assessment, monitoring may include system and network logs, email metadata, internet use, access-control logs, CCTV, site security systems, telephone records, Company vehicle telematics/GPS, time and attendance records, device security events, audit logs and use of authorised

business applications. Access to communication content, audio recording, biometric monitoring, keystroke monitoring, screenshots or similarly intrusive techniques will require a specific documented justification and enhanced approval.

6. Governance Before Monitoring Starts

- The business owner must define the specific purpose and explain why monitoring is necessary.
- HR, IT/Security and Data Protection must consider whether a less intrusive method could achieve the same purpose.
- A lawful basis must be identified. Where special category or criminal offence data is likely to be processed, the additional statutory condition and any required Appropriate Policy Document must be identified.
- A Data Protection Impact Assessment (DPIA) must be completed where monitoring is likely to result in a high risk. A DPIA should also be considered for other significant monitoring and the decision documented.
- Workers and, where appropriate, recognised representatives should be consulted before introducing significant routine monitoring unless there is a documented reason why consultation is inappropriate.
- The relevant privacy information must be issued or updated before monitoring begins.

7. Transparency and Worker Information

Workers will normally be told what is monitored, the purpose, the categories of information collected, how it may be used, who may access it, how long it is retained and their rights. Appropriate notices or signage will be used for CCTV and other location-based monitoring. Changes to monitoring arrangements will be communicated before implementation where practicable.

8. Email, Messaging and Internet Monitoring

The Company will distinguish, where practicable, between communications metadata and content. Routine security monitoring should avoid reading content unless necessary for the defined purpose. Access to mailbox or message content must follow the Access to Employee Email Accounts Policy and any applicable investigation, legal hold or business continuity process. Particular care must be taken with communications likely to contain legally privileged material, health information, trade union communications or other special category data.

9. CCTV, Audio, Location and Vehicle Monitoring

- CCTV must have a documented purpose and must not be used in areas where individuals reasonably expect privacy, such as toilets or changing facilities.
- Audio recording is more intrusive than video and will not be used routinely. It requires a specific necessity assessment and approval.
- Vehicle tracking may be used for safety, security, route/service management, asset protection or compliance. Private use and out-of-hours tracking must be restricted or disabled where not necessary.
- Monitoring of home workers must avoid unnecessary capture of household members, private living spaces or activities outside working time.

10. Biometric and AI-Assisted Monitoring

Biometric time, attendance or access controls and AI-assisted monitoring can create high data protection risk. They must not be introduced without Data Protection, HR and IT/Security approval, a DPIA where required, a clear lawful basis and any special category condition. Monitoring tools must not make solely automated or materially determinative employment decisions unless the use is lawfully approved and appropriate safeguards, including meaningful human review, are in place.

11. Covert Monitoring

Covert monitoring will not be used routinely. It may only be considered in exceptional circumstances where there are reasonable grounds to suspect criminal activity or equivalent serious misconduct, informing the individual would prejudice prevention or detection, and the monitoring is necessary and proportionate. Covert

monitoring requires senior management authorisation, HR/Data Protection involvement and a DPIA. It must be tightly targeted, time-limited and stopped when the investigation ends. Covert audio or video monitoring must not be used in areas where workers reasonably expect privacy.

12. Use of Monitoring Information

Information obtained through monitoring may be used only for the stated purpose or a compatible lawful purpose. It may be used in an investigation, disciplinary, grievance, capability, safety, fraud or legal process where relevant, accurate and fairly obtained. Monitoring data must not be treated as conclusive without appropriate human review and consideration of context.

13. Access, Disclosure, Retention and Security

Access will be restricted to authorised persons with a genuine need to know. Monitoring information will be stored securely and retained only for as long as necessary under the Group retention schedule or an applicable legal hold. External disclosure will only occur where there is a lawful basis, for example to law enforcement, regulators, insurers, professional advisers, clients where contractually justified, or in legal proceedings.

14. Individual Rights and Complaints

Individuals may exercise their data protection rights, including access to personal data obtained through monitoring, subject to statutory exemptions. Questions or complaints should be raised with HR or the Data Protection lead. Data protection complaints will be handled under the Group Data Protection Policy and complaints procedure. No person will be disadvantaged for raising a genuine concern about unlawful or disproportionate monitoring.

15. Breaches

Unauthorised monitoring, misuse of monitoring data, attempting to evade lawful security controls, or accessing monitoring information without authority may result in disciplinary or contractual action and, where appropriate, referral to regulators or law enforcement.

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.*