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", "us", "our").

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 safety, quality, effective collaboration and our reputation as a trusted industry leader.

Everyone working for or on behalf of the Company must act with professionalism, respect and responsibility, follow Company policies and lawful instructions, and raise concerns promptly where safety, wellbeing, integrity, data or legal compliance may be at risk.

1. Purpose

This policy sets clear rules for safe, secure and professional use of personal and Company mobile phones. The controls protect road and site safety, productivity, confidential information, personal data and Company reputation.

2. Scope

This policy applies to employees, workers, contractors, agency staff and anyone using a mobile phone or mobile device while working for Statom, on Company or client premises, on site, in Company vehicles or for Company business.

3. General use

- Personal use during working time must be minimal and must not interfere with duties, supervision, communication, productivity or safety.
- Personal phones should normally be used during authorised breaks and in permitted areas.
- Company-provided phones are primarily for business use and remain Company property.
- Users must follow site, client and project restrictions, including no-phone zones.

4. Driving and operating plant or machinery

It is illegal to hold and use a hand-held phone or similar data-capable device while driving, including while stationary in traffic or supervising a learner driver, except for narrow statutory exceptions. Hands-free use can still distract a driver and does not remove the duty to remain in proper control.

- Do not hold or use a phone while driving or operating plant or machinery.
- For Company business, do not make or take calls while the vehicle or plant is moving unless an exceptional safety-critical arrangement has been specifically risk assessed and approved.
- Set navigation and audio before starting the journey. If interaction with a device is needed, stop and park safely before doing so.
- Do not use headphones or devices where they reduce situational awareness on a site or in a safety-critical area.
- The emergency-services exception does not create permission for routine business use.

5. Cameras, recording and site confidentiality

- Do not photograph, film or record people, meetings, documents, drawings, sites, security controls, plant, incidents or client information without authority.
- Do not make covert audio or video recordings of workplace conversations or meetings unless there is a lawful, exceptional and approved reason.
- Respect client, principal contractor, security and intellectual-property restrictions.
- Report accidental capture or disclosure of personal or confidential information immediately.

6. Data and cyber security

- Use screen lock, strong authentication and device encryption where required.
- Do not store Company information in personal apps, personal cloud accounts or unapproved messaging services.
- Report a lost, stolen, damaged or compromised Company phone immediately to IT and the line manager.

- Do not disable security controls or install unauthorised software on Company devices.

7. Monitoring and privacy

The Company may monitor Company-provided devices and associated systems where lawful, necessary, proportionate and transparent. Monitoring will follow the Data Protection Policy, privacy notices and IT Policy. The Company will not rely on a blanket statement of “no privacy” to justify excessive monitoring.

8. Return, damage and charges

Company phones and accessories must be returned when requested, when the role no longer requires them or when employment/engagement ends. Loss, damage, fines or charges may only be recovered from pay where there is a clear lawful contractual or written authority and the deduction is otherwise permitted by law.

9. Non-compliance

Serious or repeated breach may result in removal of device privileges, disciplinary action, termination of engagement or referral under safety, data protection or legal procedures. Any decision will consider the facts, evidence, seriousness and applicable employment status.

Authorisation and review

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.