



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 standards for responsible use of social media and online platforms where use may affect Statom, its people, clients, projects, confidential information, legal obligations or reputation. It protects legitimate personal expression while setting clear work-related boundaries.

2. Scope

This policy applies to employees, workers, contractors, subcontractors and representatives. It applies to business and personal social media use where there is a connection with work, including LinkedIn, Facebook, Instagram, TikTok, X, YouTube, forums, blogs, messaging groups and similar platforms.

3. Personal expression and work connection

Employees may express lawful personal views. However, personal accounts do not remove workplace obligations where posts identify Statom, colleagues, clients, sites or projects, disclose confidential information, amount to harassment or discrimination, undermine safety or create a sufficiently close work-related impact. A disclaimer such as "views are my own" does not remove responsibility for the content.

4. Business social media

- Only authorised people may post, respond to media enquiries, make Company statements or manage official accounts.
- Marketing and project content must use approved information, branding and permissions.
- Do not publish client, project, tender, commercial, financial, technical or security information without authority.
- Obtain appropriate consent or authority before posting identifiable images of workers or third parties.

5. Prohibited conduct

- Discrimination, harassment, sexual harassment, victimisation, threats, bullying, hate content or targeted abuse connected with work.
- Disclosure of confidential, personal, commercially sensitive, security-sensitive or legally privileged information.
- False or misleading statements presented as Company information.
- Posting site photographs, drawings, access arrangements, incidents or client information contrary to project or security restrictions.
- Impersonating the Company, colleagues or clients or creating unauthorised official-looking accounts.
- Retaliating online against someone who has raised a grievance, harassment complaint or protected disclosure.

6. Personal data, photographs and recordings

Personal data shared through social media remains subject to data protection law. Employees must not post personal information, images or recordings obtained through work unless authorised and lawful. Screenshots, private-group content and direct messages may still create data protection, confidentiality or conduct issues.

7. Social media and recruitment / employment decisions

Managers must not carry out informal social-media screening of applicants, employees or workers for recruitment, promotion, disciplinary or performance purposes unless an approved process, lawful basis,

transparency and equality safeguards are in place. Any monitoring or investigation must be necessary, proportionate and coordinated with HR and the Data Protection Lead.

8. Monitoring

Statom may monitor use of Company systems and may review publicly available online material where there is a legitimate work-related reason, but only where lawful, necessary and proportionate. Monitoring must comply with the Data Protection Policy and applicable privacy information; excessive or indiscriminate monitoring is prohibited.

9. Reporting and removal

Employees should report suspected leaks, impersonation, harassment, threats, security concerns or inappropriate work-related posts to their manager, HR, IT or the Data Protection Lead as appropriate. The Company may require removal or correction of content where it breaches law, confidentiality, security, intellectual property, contractual duties or this policy, subject to the circumstances and applicable rights.

10. Whistleblowing and protected activity

Nothing in this policy prevents lawful protected disclosures, reporting criminal conduct, contacting prescribed regulators, seeking legal advice, reporting health and safety risks or exercising statutory rights. Employees should avoid unnecessary disclosure of confidential or personal information beyond what is reasonably required for the protected purpose.

11. Non-compliance

Potential breaches will be assessed under the relevant process and in context. Serious disclosure, harassment, threats, discriminatory conduct, deliberate reputational harm, cyber security breaches or retaliation may amount to gross misconduct. Contractors or third parties may have access or engagement restricted or terminated.

12. Related policies

- Information Technology Policy
- Mobile Phone Policy
- Data Protection, GDPR and Cyber Security Policy
- Bullying, Harassment and Sexual Harassment Policy
- Equal Opportunities, Diversity and Inclusion Policy
- Whistleblowing Policy
- Disciplinary Policy

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.*