



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 the rules for secure, lawful and responsible use of Statom information technology, communication systems, devices, networks, software, data and digital tools. It supports cyber security, data protection, business continuity, client assurance and professional conduct.

2. Scope

This policy applies to anyone who uses or accesses Statom IT resources or information, including employees, workers, directors, contractors, consultants and agency staff. It applies to Company devices, approved personal devices, email, Microsoft 365, cloud services, collaboration tools, site systems, mobile devices, removable media and artificial intelligence tools used for Company business.

3. Core controls

- Use systems only for legitimate, authorised purposes.
- Protect credentials, confidential information and personal data.
- Use multi-factor authentication and approved password controls where required.
- Use only IT-approved devices, software, applications, cloud services and storage.
- Report phishing, loss, theft, unusual access, malware, misdirected information and suspected breaches immediately.
- Do not bypass security controls, install unauthorised software or share accounts.

4. Email, messaging and internet

- Use Company email, Teams and approved channels professionally and check recipients and attachments before sending.
- Do not auto-forward Company email to personal accounts.
- Do not use personal email, consumer cloud storage or unapproved messaging platforms for confidential Company, client, payroll, HR or project information.
- Do not access, create, store or distribute unlawful, discriminatory, harassing, sexually explicit, extremist, defamatory, fraudulent or malicious content using Company systems.
- Limited personal use may be permitted where reasonable, lawful, secure and non-disruptive.

5. Access management

- Access is role-based and limited to what is required for authorised duties.
- Users must not access HR, payroll, commercial, client, email or employee data without a legitimate business need and authority.
- Managers must notify IT promptly of starters, movers, leavers and role changes.
- Administrator and privileged access must be restricted, approved, logged and reviewed.
- Access to another employee's mailbox must follow the Access to Employee Email Accounts Policy.

6. Devices, BYOD and remote work

- Company devices remain Company property and must be protected from loss, theft, damage and unauthorised viewing.

- Personal devices may only be used for Company business with IT approval and required controls, including encryption, screen lock, MFA, security updates and remote wipe where appropriate.
- Remote access must use approved secure methods. Public Wi-Fi must not be used for sensitive work unless an approved secure connection is in place.
- Company data must not be stored on personal devices or removable media unless expressly authorised.
- Lost, stolen or compromised devices must be reported immediately.

7. Software, licensing and updates

- Only approved, licensed and supported software may be installed or used.
- Security updates and patches must be applied in line with IT instructions.
- Unsupported, pirated, cracked or unauthorised software, scripts, extensions and tools are prohibited.
- Users must not disable endpoint protection, filtering, logging, mobile device management or other security controls.

8. Artificial intelligence and automated tools

Employees must not enter confidential, personal, client, commercially sensitive, legally privileged or security-sensitive information into public or unapproved AI tools. AI-enabled systems used for HR, recruitment, payroll, monitoring, performance, access, safety or disciplinary decisions require prior HR, IT and Data Protection Lead approval, appropriate risk assessment, transparency and meaningful human oversight where required by law.

9. Data protection and monitoring

IT use may be monitored where lawful, necessary, proportionate and transparent for security, safety, compliance, investigation, quality and business continuity. Monitoring is not justified merely because it is technically possible. The Company will identify a lawful basis, provide appropriate privacy information and complete a DPIA where required. Covert monitoring will only be used exceptionally and lawfully.

10. Cyber and data incident response

- Report incidents immediately to IT and the Data Protection Lead; involve HR where employee or HR data is affected.
- Do not investigate alone, delete evidence, alter logs or conceal an incident.
- Follow containment instructions, including password resets, isolation, access suspension or device return.
- Personal data breaches will be assessed and recorded under the Data Protection Policy, including the 72-hour ICO notification test where applicable.

11. Leavers and return of assets

On termination or when requested, users must return Company devices, storage media, access tokens and other IT assets, and must not retain Company information. IT will disable or amend access in line with the joiner/mover/leaver process, legal holds and retention requirements.

12. Non-compliance

Unauthorised access, deliberate data loss, credential sharing, cyber security breaches, misuse of systems, circumvention of controls or serious confidentiality breaches may result in disciplinary action up to and including dismissal, termination of engagement, access suspension, contractual remedies or referral to authorities.

13. Related policies

- Data Protection, GDPR and Cyber Security Policy
- Subject Access Request (SAR/DSAR) Policy and Procedure
- Access to Employee Email Accounts Policy
- Access to Personal Data Policy
- Mobile Phone Policy
- Social Media Policy
- Flexible Working 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.*