



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 governs internal access to personal data held by Statom. It ensures that personal data is accessed only by authorised people for legitimate business purposes, with appropriate security, confidentiality, audit and data protection controls. It does not govern an individual's right to request a copy of their own personal data; that process is set out in the SAR/DSAR Policy and Procedure.

2. Scope

This policy applies to employees, workers, directors, contractors, consultants, agency staff and third-party service providers who access or may access personal data processed by Statom, including HR, payroll, recruitment, health, CCTV, access-control, IT, email, client, supplier and site records.

3. Legal framework

- UK GDPR.
- Data Protection Act 2018.
- Data (Use and Access) Act 2025, as in force.
- Common-law and contractual confidentiality duties.
- Relevant employment, equality, health and safety, tax, immigration, regulatory and legal-claims requirements.

4. Access principles

- Need to know: access only where required for authorised duties.
- Least privilege: give the minimum level of access necessary.
- Purpose limitation: use data only for the approved purpose unless a lawful compatible purpose applies.
- Data minimisation: access and extract only what is necessary.
- Confidentiality and security: protect information from unauthorised viewing, disclosure, alteration or loss.
- Accountability: approvals, searches and exceptional access must be capable of audit where appropriate.

5. Standard role-based access

System and folder access must be based on role, responsibility and business need. Managers must not grant informal access by sharing passwords, forwarding confidential data to personal accounts or using shared credentials. IT and system owners must review access when people join, move role, change responsibility or leave.

6. Sensitive categories

Access to special category data, criminal-offence data, health records, occupational health information, disciplinary and grievance material, whistleblowing information, payroll, bank details, right-to-work evidence and legal advice requires enhanced care and restricted access. Legal privilege must be preserved.

7. Access to another person's email, files or account

Access to another employee's email account must follow the Access to Employee Email Accounts Policy. Access to OneDrive, Teams, local folders or other individual workspaces must be authorised for a defined purpose,

limited in scope and duration, and logged where technically available. Targeted retrieval should be used before broad access wherever practicable.

8. Investigations, litigation and legal holds

Where access is required for an investigation, grievance, disciplinary matter, whistleblowing concern, legal claim, audit, safeguarding matter or regulatory request, HR, Legal, IT or the Data Protection Lead will define the purpose and scope. Relevant records must be preserved and must not be deleted, altered or concealed.

9. Data subject requests and complaints

Any request by an individual for access to their own personal data must be escalated immediately under the SAR/DSAR Policy. Any complaint about how personal data is handled must be forwarded to the Data Protection Lead without delay. The Company will maintain the legally required complaints route, acknowledge data protection complaints within 30 days and respond without undue delay.

10. Third-party and processor access

- Complete appropriate due diligence before granting a supplier or processor access.
- Use written contracts and documented instructions.
- Restrict access to named or role-defined personnel where appropriate.
- Apply suitable confidentiality, security, sub-processor, audit, breach and return/deletion controls.
- Remove access promptly when the purpose ends.

11. Monitoring and audit

The Company may audit access logs and investigate suspected unauthorised access where lawful, necessary and proportionate. New monitoring arrangements require Data Protection Lead and IT review and a DPIA where required.

12. Non-compliance

Browsing records without business need, sharing credentials, disclosing data without authority, deliberate misuse, concealment, deletion or unauthorised extraction may amount to gross misconduct and may lead to access suspension, disciplinary action, termination of engagement, regulatory reporting or legal action.

13. Related policies

- Data Protection, GDPR and Cyber Security Policy
- Subject Access Request (SAR/DSAR) Policy and Procedure
- Access to Employee Email Accounts Policy
- Information Technology Policy
- Disciplinary Policy
- Whistleblowing Policy
- Data Retention Schedule

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.*