



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 governs access to a work email account by anyone other than the account holder. It supports business continuity, legal and regulatory compliance, investigations, information security and protection of Company records while respecting privacy and data-protection rights.

2. Scope

This policy applies to employees, workers, directors, agency workers, contractors and consultants with a Company email account, and to all Company-managed mailboxes, archives, backups, devices and access methods.

3. Legal and privacy framework

Mailbox access and email monitoring must comply with the UK GDPR and Data Protection Act 2018 as amended, including changes made by the Data (Use and Access) Act 2025, together with the Human Rights Act 1998, confidentiality obligations and applicable employment law. Access must be lawful, necessary, proportionate, transparent where required and limited to a defined purpose.

4. Core controls

- targeted retrieval before broad mailbox access wherever practicable
- least-privilege access for named individuals only
- documented business purpose and authorisation
- defined start and end dates
- audit logging and secure handling
- segregation of privileged, health, trade-union, whistleblowing and other particularly sensitive communications where appropriate
- no access for curiosity, convenience, personal disputes or fishing expeditions

5. Roles and responsibilities

Role	Responsibility
Requester	Provide a written business reason, scope, alternatives considered and required duration.
HR	Confirm employment status, fairness, policy alignment and employment-law considerations.
IT / IT Provider	Implement access securely, apply time limits, preserve logs and remove access promptly.
Data Protection Lead /	Advise on high-risk access, monitoring, sensitive data, investigations, DPIAs

DPO	and legal restrictions.
Authorising Director	Approve exceptional, non-consensual or high-risk access where required.

6. Permitted purposes

- urgent business continuity during absence or incapacity
- operational handover, long-term leave or role change
- legal hold, litigation, regulatory request or subject access response
- investigation of suspected misconduct, fraud, harassment, security incident or data loss
- protection of confidential information, intellectual property, client obligations or Company assets

7. Current workers - operational access

For ordinary holiday, short absence or handover, managers should use delegation, shared mailboxes or targeted retrieval wherever possible. Where appropriate, the employee should be informed in advance and the scope and duration agreed. Consent is not treated as the sole legal basis for processing because of the imbalance inherent in the employment relationship.

8. Access without prior notice

Access without prior notice may only be authorised where notice cannot reasonably be given, would prejudice a legitimate investigation, would create a material security risk, or a pressing legal or regulatory requirement applies. The decision must record the lawful basis, necessity, scope, duration and whether and when the individual should later be informed.

9. Former workers and leavers

Business emails and records remain Company records subject to retention and legal-hold requirements. On exit, IT will disable personal access promptly, apply an appropriate auto-reply or controlled forwarding arrangement where authorised, retain the mailbox in line with the retention schedule and delete it when the retention period expires unless preservation is required.

10. Monitoring of email content

Routine unrestricted reading of employee email content is not permitted. Where systematic or content-based monitoring is proposed, the Company must define the purpose, assess whether less intrusive measures would achieve it, provide appropriate privacy information and complete a Data Protection Impact Assessment where required. Covert monitoring will only be considered in exceptional circumstances, for a strictly limited period and with senior HR, IT and Data Protection approval.

11. Approval levels

Access type	Minimum approval
Current worker - routine operational access	HR + IT; employee informed where appropriate
Current worker - without prior notice	HR + Authorising Director + IT
High-risk / broad search / sensitive case	HR + Authorising Director + Data Protection Lead/DPO + IT
Former worker - targeted retrieval	HR confirmation + IT
Legal hold / dispute / investigation involving leaver	HR + Director + Data Protection / Legal + IT

12. Special communications

Access requests must consider whether the mailbox may contain communications with legal advisers, trade union representatives, occupational health, whistleblowing channels, safeguarding contacts or other confidential or special-category information. Such material must not be accessed, used or disclosed beyond what is strictly lawful and necessary.

13. Employee communications

The Company will inform individuals about the nature and purposes of monitoring and mailbox-access practices through this policy, the Employee Privacy Notice and related IT policies. Specific access may be notified before or after the event unless doing so would prejudice an investigation or conflict with a legal obligation.

14. Minimum request record

- Group Company and requester
- mailbox owner and employment status
- business purpose and justification
- date range, keywords, folders or other scope
- named individuals needing access
- start and end dates
- alternatives considered
- HR approval
- investigation, legal hold or sensitive-data flag

15. Non-compliance

Unauthorised mailbox access, misuse of retrieved content or failure to follow this policy may result in disciplinary action, contract action and/or legal or regulatory consequences.

16. Related policies

- Data Protection, GDPR & Cyber Security Policy
- Employee Monitoring Policy
- Access to Personal Data Policy
- Subject Access Request (SAR/DSAR) Policy and Procedure
 - Employee Privacy Notice
- IT and Communications / Acceptable Use Policy
- Information Security Policy
- Records Retention Schedule
- Whistleblowing Policy
- Disciplinary Policy

17. Review

The Group Chief People Officer, IT and Data Protection Lead will review this policy annually and whenever relevant data-protection or monitoring guidance changes.

AUTHORISED AND SIGNED

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.*