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. Introduction

Statom Group is committed to protecting all personal data and digital assets in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA). We have achieved Cyber Essentials Plus certification to demonstrate our implementation of recognised cyber security controls and our commitment to safeguarding stakeholder data.

This policy sets out our approach to:

- Legal and regulatory compliance
- Accountability and data governance
- Cyber security and system integrity
- Data subject rights and access
- Breach response and risk management

2. Scope

This policy applies to all:

- Employees
- CIS contractors and subcontractors
- Consultants and agency workers
- Suppliers and authorised third parties

It covers all personal and business-critical data, whether processed digitally or manually, and applies to work conducted on behalf of Statom Group regardless of physical location or device used.

3. Legal & Regulatory Compliance

Statom Group complies with the following legislation and frameworks:

- UK GDPR (as amended)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations 2003 (as amended)
- ICO guidance and enforcement notices
- Cyber Essentials Plus
- ISO 27001-aligned principles (where applicable)

We monitor emerging legislation and regulatory advice to ensure ongoing compliance.

Key Definitions

Term	Definition
Personal Data	Information relating to an identifiable individual.
Data Subject	The individual whose data is being processed.
Processing	Any operation performed on personal data, including collection, storage, access, or destruction.
Data Controller	Statom Group, who determines the purposes and means of processing.
Data Processor	A third party who processes data on our behalf.
Cyber Essentials Plus	Government-backed certification evidencing effective protection against common cyber threats.

4. Data Protection Principles

We uphold the seven principles under Article 5 of UK GDPR and DUAA 2025:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

5. Types of Data Processed

We may process the following categories of personal data:

- Contact and employment information
- Payroll and financial data
- Health, medical or absence records
- Disciplinary, grievance or performance records
- Training and development records
- Recruitment and equal opportunity monitoring data

We only process special category data where required by law or for legitimate business purposes, with safeguards in place.

6. Data Subject Rights

We fully recognise and support individual rights, including those expanded under the DUAA 2025:

- Right to be informed
- Right of access (including proportional searches and stop-the-clock mechanisms)
- Right to rectification
- Right to erasure ("right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object

- Rights related to automated decision-making, including human review and explanation

Requests will be responded to within one calendar month, with identity verification and proportionality assessment as required by law.

7. Data Security & Cyber Essentials Plus

We employ layered cyber and information security measures, including administrative, physical, and technical controls.

8. Scope of Certification

Covers:

- Company-managed desktops, laptops, mobile devices
- Office 365, SharePoint, Chime, FieldView
- Websites, portals and cloud-based file-sharing systems

9. Technical Controls

Area	Implementation
Firewalls	Centrally managed, reviewed quarterly
Secure Configuration	Auto-lock, least-privilege settings, regular audits
Access Control	Admin access reviewed and restricted
Malware Protection	Real-time protection and central oversight
Software Updates	Weekly patching, monitored by Head of IT

10. Data Handling and Retention

- Personal data is retained only as long as necessary for its original purpose.
- Access is restricted to authorised personnel only.

All staff must:

- Use strong passwords and auto-lock settings
- Avoid using unauthorised storage systems
- Report any suspected breach or misdirected email immediately

11. Data Breaches

We operate a clear and prompt breach management protocol. Statom Group will:

- Record and investigate all incidents and near misses
- Notify the Information Commissioner's Office (ICO) within 72 hours where legally required
- Inform affected individuals without undue delay if there is a high risk to rights and freedoms

12. International Data Transfers

Statom Group does not currently transfer data outside the UK. If this changes, transfers will only be permitted:

- Under UK Government adequacy regulations, or
- With appropriate safeguards such as the UK International Data Transfer Agreement (IDTA) or Standard Contractual Clauses (SCCs)

13. Data Protection Governance

- A full Record of Processing Activities (ROPA) is maintained.
- Data Protection Impact Assessments (DPIAs) are carried out for high-risk or innovative data uses.
- Annual data protection training is mandatory for all staff.
- Quarterly risk and asset reviews are conducted by the IT Systems Manager.

14. Access Requests and Disclosures

- Access requests must be submitted in writing.
- Requests will be responded to within one calendar month, with the option to extend in line with DUAA proportionality clauses.

Personal data will only be disclosed:

- Where required by law
- For specific, legitimate business functions (e.g. payroll, health & safety)
- In accordance with the data minimisation principle

15. Roles & Responsibilities

Role	Responsibility
Senior Management	Policy oversight, strategic direction, resourcing
Data Protection Officer (DPO)	Legal compliance, breach management, access request coordination
Head of IT	Cyber security, patching, access control, audit readiness
All Employees & Contractors	Following policies, protecting data, reporting concerns

16. Review and Updates

This policy will be reviewed annually or following any relevant legislative, regulatory or operational change. Any material changes will be communicated to all staff, contractors, and relevant third parties.

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

This policy is subject to annual review and approval by the Board.