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

This Information Technology (IT) policy sets out the guidelines and procedures for the use of IT resources at Statom Group Ltd. The purpose of this policy is to ensure the secure, efficient, and responsible use of the company's IT systems and to comply with relevant UK legislation.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at Statom Group Ltd who use the company's IT resources. It covers all company-owned, leased, or rented hardware, software, networks and information systems.

3. Acceptable Use

3.1. General Use

- IT resources are provided to support the business activities of Statom Group Ltd.
- Personal use of IT resources should be minimal and must not interfere with work responsibilities.
- Users must ensure that their use of IT resources does not expose the company to security risks, legal liabilities, or reputational damage.

3.2. Email and Communication Systems

- Company email accounts should be used for business purposes only.
- Users must not send or forward emails containing inappropriate content, such as offensive language, harassment, or confidential information without authorization.
- Phishing attempts and suspicious emails should be reported immediately to the IT department.

3.3. Internet Use

- The internet should be used primarily for work-related activities.
- Accessing, downloading, or distributing illegal, offensive, or inappropriate content is strictly prohibited.
- Users must not engage in activities that could compromise network security, such as accessing unauthorised sites or downloading unapproved software.

4. Security and Data Protection

4.1. Password Management

- All users must use strong passwords that are regularly updated. Passwords should be unique and not shared with others.
- Passwords must be kept confidential and stored securely.

4.2. Data Protection

- Users must comply with the UK GDPR and Data Protection Act 2018, ensuring that personal data is processed lawfully, transparently, and securely.
- Personal data should only be accessed, shared, or stored as necessary for the performance of job duties.
- Data breaches must be reported immediately to the Data Protection Officer (DPO).

4.3. System Access and Usage

- Access to company systems and information is granted based on job role and responsibilities.
- Users are prohibited from accessing or attempting to access systems, files, or data that they are not authorized to use.
- Remote access to company systems is permitted through secure methods approved by the IT department.

4.4. Antivirus and Software Updates

- All company devices must run approved antivirus software and receive regular updates.
- Users must not install unapproved or pirated software on company devices.
- Software updates and patches must be applied promptly to maintain system security.

5. Hardware and Software Management

5.1. Hardware

Rules:

1. No equipment should be moved without the consent of the IT Department.
2. No equipment may be attached to the network without IT Department approval.
3. Equipment must not be modified without IT Department consent.
4. Equipment must be treated with care and maintained properly. Any faults, losses, or damage should be reported to IT immediately.
5. All equipment should be logged off and powered down when not in use for extended periods.
6. Laptops must be secured when taken off-site. They should not be left unattended and must be protected from theft.

Personal Devices: Personal devices may only be used for work purposes if approved by the IT department and configured according to company security standards.

5.2. Software

- All software used on company systems must be properly licensed and approved by the IT department.
- Users are prohibited from copying, distributing, or installing software without authorization.
- Under no circumstances may users purchase or load software without Company approval.

6. Monitoring and Compliance

6.1. Monitoring

- Statom Group Ltd reserves the right to monitor IT resource usage to ensure compliance with this policy. This includes monitoring emails, internet usage, and access to files and systems.
- Monitoring will be conducted in accordance with UK law, including the Investigatory Powers Act 2016.

6.2. Compliance

- Failure to comply with this IT policy may result in disciplinary action, including termination of employment or contract.
- Users who suspect a breach of this policy must report it immediately to their manager or the IT department.

7. Training and Awareness

- All employees will receive regular training on IT security, data protection, and the responsible use of IT resources.
- Users are encouraged to stay informed about current IT security threats and best practices.

8. Review and Updates

- This policy will be reviewed annually or as necessary to ensure it remains relevant and compliant with UK law.
- Any updates to the policy will be communicated to all users promptly.

9. Contact Information

For questions or concerns regarding this policy, please contact the IT Department.

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.