



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 ensures that paper records, electronic storage media and devices are securely sanitised, destroyed or disposed of when no longer required, so confidential information and personal data cannot be recovered or disclosed unlawfully.

2. Scope

This policy applies to employees, workers, contractors and approved third parties handling Statom records, devices or storage media. It covers HDDs, SSDs, USB/flash media, memory cards, tapes, optical media, mobile devices, laptops, servers, printers/copiers, network devices, paper files and any equipment capable of retaining data.

3. Legal and security framework

- UK GDPR and Data Protection Act 2018 requirements for storage limitation, integrity/confidentiality and appropriate security.
- Data (Use and Access) Act 2025 as commenced and applicable.
- Statom Data Protection, GDPR & Cyber Security Policy and retention schedule.
- NCSC secure sanitisation principles and recognised secure-destruction practices appropriate to the sensitivity of the information.
- Environmental and WEEE obligations where electronic equipment is disposed of.

4. Retention comes first

Records must not be destroyed merely because they are inconvenient, old or connected with a dispute. Before destruction, the responsible owner must confirm that the applicable retention period has expired and that no legal hold, investigation, SAR/DSAR, grievance, tribunal claim, audit, insurance, regulatory or contractual preservation requirement applies.

5. Classification and method selection

The disposal method must reflect the type of media, sensitivity of the information, whether the media will be reused, the capability of the technology and the risk if data were recovered. Ordinary deletion or quick formatting is not sufficient for sensitive data.

Media / situation	Approved approach
Paper records	Cross-cut shredding or approved confidential-waste destruction; never general waste where confidential or personal data is present.
Reusable electronic media	Use an IT-approved secure sanitisation method suitable for the media and verify completion before reassignment or release.
SSDs / flash storage	Use manufacturer/NCSC-aligned sanitisation or cryptographic erase where appropriate; physical destruction may be required where assurance cannot be achieved.

Magnetic media	Approved secure erase or suitable degaussing where technically effective; otherwise physical destruction.
Devices leaving Company control	Sanitise before sale, donation, return, repair or disposal; revoke credentials/certificates and remove Company identifiers where appropriate.
Failed or inaccessible media	Treat as containing data and use secure physical destruction unless IT can verify effective sanitisation.

6. Authorisation and chain of custody

- IT must authorise disposal of Company electronic assets and record asset identifiers where applicable.
- Records owners/HR/Finance/Legal must authorise destruction of sensitive paper records in accordance with the retention schedule.
- Media awaiting destruction must be stored securely with restricted access.
- Transfers to third-party destruction providers must use controlled collection and chain-of-custody arrangements.

7. Third-party destruction providers

Providers must be appropriately vetted and contractually required to protect confidentiality, security, subcontracting and disposal. Statom should use recognised secure destruction standards appropriate to the risk and obtain a Certificate of Destruction or equivalent evidence. Supplier failures affecting personal data must be escalated as potential data breaches.

8. Evidence and destruction log

Where proportionate, the disposal record should identify the asset or record set, owner, authoriser, date, method, provider, certificate reference and any exception. Evidence must be retained for audit in line with the retention schedule.

9. Personal devices and BYOD

Where an approved personal device has stored or accessed Company information, IT may require removal of Company data, revocation of access, remote wipe of the Company container or other controls when the device is lost, replaced, the arrangement ends or the user leaves. Personal data unrelated to Statom must not be accessed or erased beyond what is necessary and lawful.

10. Incidents and non-compliance

Lost media, disposal in general waste, missing destruction evidence, unauthorised sale/reuse or suspected recoverability of confidential data must be reported immediately to IT and the Data Protection Lead. Deliberate or serious breaches may result in disciplinary or contractual action.

11. Related policies

- Data Protection, GDPR & Cyber Security Policy
- IT Policy
- Access to Personal Data Policy
- Subject Access Request (SAR/DSAR) Policy and Procedure
- Records Retention Schedule
- Leaver and asset-management procedures

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.*