Data Protection & GDPR Policy

HR-POL-026-02

1. Introduction

Statom Group is committed to protecting personal data and digital infrastructure in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025. In support of this commitment, we have achieved Cyber Essentials Plus certification to demonstrate robust protection against common cyber threats and to safeguard our stakeholders' data.

This policy sets out how Statom Group protects both personal data and digital systems, including our approach to legal compliance, accountability, cyber security controls, data breach response, and ongoing risk management.

2. Scope

This policy applies to all Statom Group employees, contractors, subcontractors, consultants, agency workers, suppliers and any authorised third parties who process or access personal or business-critical data or use Statom-controlled systems and networks.

It covers both digital and manual data, all IT devices, applications, websites, and any work conducted on behalf of Statom Group, regardless of location.

3. Legal & Regulatory Compliance

Statom Group complies with the following:

- UK GDPR (as amended)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications Regulations (PECR) 2003 (as amended)
- ISO-aligned security principles and the Cyber Essentials Plus scheme

We also comply with any obligations issued by the Information Commission (formerly ICO), the UK supervisory authority for data protection.

4. Key Definitions

Term	Definition
Personal Data	Information identifying an individual (e.g., name, address, contact details).
Data Subject	The individual whose data is being processed.
Processing	Operations such as collecting, storing, using, or deleting personal data.
Data Controller	Statom Group, which determines how and why data is processed.
Data Processor	A third party that processes personal data on our behalf.

Cyber Essentials Plus *- A UK Government-backed certification confirming baseline cyber protections have been implemented and independently verified.*

5. Data Protection Principles

We uphold the following principles as set out in Article 5 of the UK GDPR and the DUA Act:

- Lawfulness, Fairness, and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

6. Types of Data Processed

We may process the following types of personal data:

- Contact details, employment information, payroll data, next of kin, and job role
- Health and medical information
- Disciplinary, performance, and training records
- Recruitment and equal opportunity monitoring data

Special category data, such as health or ethnicity, is only processed when necessary to comply with legal obligations or equality monitoring requirements.

7. Data Subject Rights

Statom Group recognises the rights of individuals under data protection law:

- Right to be informed
- Right of access (responded to within one calendar month)
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision-making and profiling

8. Data Security & Cyber Essentials Plus

We protect data using administrative, physical, and technical controls. Statom Group achieved Cyber Essentials Plus certification to confirm our protections against common cyber threats.

8.1 Scope of Cyber Essentials Plus Certification

Includes:

- Laptops, desktops, tablets, Mobile devices
- Office 365, SharePoint, FieldView, Chime
- Company websites, portals, and file-sharing systems

8.2 Core Technical Controls

Area	Implementation
Firewalls	Centrally managed with strict traffic rules
Secure Configuration	Unused services removed; auto-lock screens enabled
Access Control	Admin privileges restricted and reviewed regularly
Malware Protection	Real-time endpoint protection across all devices
Software Updates	OS and applications patched automatically and tracked weekly

9. Data Handling and Retention

Data is retained only as long as necessary for its intended purpose. Personal data is stored securely, with access limited to authorised personnel.

All employees must:

- Avoid storing data in personal email or unauthorised systems
- Use strong passwords and enable screen locks
- Report any suspected breach immediately

10. Data Breaches

Statom Group will:

- Record and investigate all data breaches or near misses
- Notify the Information Commission within 72 hours if a notifiable breach occurs
- Notify affected individuals without undue delay if there is a high risk to their rights and freedoms

11. International Data Transfers

We do not currently transfer data outside the UK. If future transfers occur, they will be governed by:

UK Government adequacy regulations; or

Approved safeguards such as the UK International Data Transfer Agreement (IDTA) or Standard Contractual Clauses (SCCs)

12. Data Protection Governance

- Records of Processing Activities (ROPA) are maintained in compliance with Article 30 UK GDPR.
- Data Protection Impact Assessments (DPIAs) are carried out for high-risk processing activities.
- Staff training is provided at induction and refreshed annually.
- Cyber risk and asset reviews are conducted quarterly by the IT Manager.

13. Access Requests and Disclosures

Data subjects can request access to their personal data free of charge. Requests will be responded to within one calendar month.

Personal data will only be disclosed:

- Where legally required
- For legitimate purposes such as payroll, HR, health and safety, or insurance
- In line with the data minimisation principle

14. Roles & Responsibilities

Role	Responsibility
Senior Management	Governance, oversight, policy review, funding
Data Protection Officer	Compliance oversight, breach response, data subject liaison
IT & Systems Manager	Device security, patching, access control, cyber essentials audits
Employees	Follow procedures, protect information, report incidents

15. Review and Updates

This policy will be reviewed annually or upon any relevant legislative or operational change. Statom Group will communicate updates to all staff and relevant partners.

SIGNED:

Martina Oyite
Human Resources Director
Statom Group Limited
REVIEW: Annual
DATE: 01/06/2025
NEXT REVIEW: 01/06/2026

SIGNED:

Paul Whelan
Managing Director
Statom Group Limited
REVIEW: Annual
DATE: 01/06/2025
NEXT REVIEW: 01/06/2026