



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 sets out how Statom protects personal data and information systems, complies with data protection law, informs individuals about how their personal data is used, and manages personal data breaches and security incidents.

The policy supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025, with all relevant data protection provisions now in force, the Privacy and Electronic Communications Regulations 2003 where relevant, ICO guidance and relevant cyber security controls, including Cyber Essentials Plus.

2. Scope

This policy applies to all personal data and business-critical information processed by Statom, whether held digitally, on paper, in email, on collaboration platforms, in HR/payroll systems, in recruitment systems, in CCTV or access systems, on mobile devices, on site systems, in vehicles or plant systems, or by authorised third parties.

- employees, workers, apprentices and directors;
- CIS contractors, subcontractors, consultants and agency workers;
- job applicants and work experience applicants;
- suppliers, clients, visitors and authorised third parties;
- all Company systems, devices, networks, applications, premises, sites, projects and approved remote working arrangements.

It applies regardless of work location, device type or system used, including site-based, office-based, remote and hybrid working.

3. Key definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable individual.
Special category data	More sensitive personal data, including health data, biometric data used for identification, racial or ethnic origin, religious or philosophical beliefs, trade union membership, political opinions, genetic data, sex life or sexual orientation data.
Criminal offence data	Personal data relating to criminal convictions, offences, allegations, proceedings or related security measures.
Data subject	The individual whose personal data is being processed.
Processing	Any operation performed on personal data, including collection, use, access, storage, sharing, amendment, deletion or destruction.

Controller	The organisation that decides why and how personal data is processed. For most employment and business processing, Statom is the controller.
Processor	A third party that processes personal data on Statom's documented instructions.
Data Protection Lead	The person or role responsible for coordinating data protection compliance. Where a statutory DPO is formally appointed, DPO responsibilities apply.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Data protection principles

Statom applies the UK GDPR principles to all personal data processing:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality;
- accountability.

5. Accountability and governance

- Maintain a Record of Processing Activities (ROPA) covering key HR, payroll, recruitment, IT, commercial, site and operational processing.
- Complete Data Protection Impact Assessments (DPIAs) before high-risk processing, new monitoring technology, new biometric systems, significant CCTV changes, AI-enabled HR tools or major system changes.
- Complete supplier due diligence before appointing processors who handle personal data.
- Put written data processing agreements in place with processors before personal data is shared.
- Review access rights, assets, risks and security controls at appropriate intervals.
- Provide mandatory data protection and cyber security training to staff and relevant contractors.
- Keep evidence of compliance decisions, risk assessments, breach assessments, training, rights request handling and privacy notice updates.

6. Lawful basis for processing

Statom must identify and document a lawful basis before processing personal data. The lawful basis depends on the purpose of processing.

Purpose	Likely lawful basis
Recruitment and selection	Legitimate interests; steps before entering into a contract; legal obligation where checks are required.
Employment contract administration	Contract; legal obligation; legitimate interests.
Payroll, tax, pensions and statutory reporting	Legal obligation; contract.
Benefits and reward administration	Contract; legitimate interests; consent only where legally required and freely given.
Absence, health, reasonable adjustments and occupational health	Legal obligation; employment law obligations; assessment of working capacity; substantial public interest where applicable; explicit consent only where appropriate.
Disciplinary, grievance, performance and investigations	Contract; legal obligation; legitimate interests; legal claims where relevant.
Health and safety, site access and incident management	Legal obligation; legitimate interests; vital interests in

	exceptional emergencies.
IT, cyber security, system monitoring and audit logs	Legal obligation; legitimate interests.
CCTV, premises security, site security, vehicle or plant tracking	Legitimate interests; legal obligation where relevant.
Legal claims and insurance	Legitimate interests; legal obligation; establishment, exercise or defence of legal claims.
Marketing, website analytics or cookies	Consent where required by PECR; legitimate interests where lawful and proportionate.

7. Special category and criminal offence data

Statom will only process special category data where it has both a UK GDPR Article 6 lawful basis and an Article 9 condition. Common employment-related conditions include employment, social security and social protection law obligations, occupational health or assessment of working capacity, substantial public interest, vital interests, explicit consent where appropriate, and establishment, exercise or defence of legal claims.

Criminal offence data will only be processed where legally permitted and necessary, for example for right to work checks, statutory vetting, site security, safeguarding, fraud prevention, investigations or legal claims. Access to this data must be restricted and retention must be justified.

8. Categories of personal data processed

- identity and contact details, including name, address, telephone number, email address, date of birth and emergency contacts;
- right to work, immigration, qualifications, licences, training and certification records;
- employment, contract, role, reporting line, salary, pay, pension, benefits, tax and bank details;
- attendance, working time, holiday, absence, family leave, occupational health and medical information;
- performance, appraisal, promotion, succession, disciplinary, grievance, investigation and exit records;
- recruitment information, including CVs, interview notes, assessment results and references;
- equal opportunity monitoring data where collected;
- IT user account information, audit logs, device data, email and system usage data;
- CCTV, premises access, site access, vehicle, plant or telematics data where used;
- supplier, subcontractor, client and visitor contact and business relationship information.

9. Privacy notices

Statom will provide appropriate privacy information at or before the point personal data is collected, unless an exemption applies. The privacy notices in Appendix 1, Appendix 2 and Appendix 3 form part of this policy. Additional local or system-specific notices may be issued where required.

Managers must not collect new categories of personal data, introduce new monitoring arrangements, use new HR technology, or change the purpose of existing processing without confirming that the relevant privacy information, lawful basis and risk assessment are in place.

10. Data subject rights and rights requests

Individuals have the following rights, subject to statutory conditions and exemptions:

- right to be informed;
- right of access;
- 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.

Rights requests may be made verbally or in writing. Statom will respond without undue delay and normally within one calendar month. Where permitted by law, Statom may pause time while waiting for information needed to clarify the request or verify identity, and may extend the response period for complex or multiple requests.

Searches for personal data must be reasonable and proportionate. The Company may refuse or charge a reasonable fee for manifestly unfounded or excessive requests, in line with applicable law and ICO guidance. The operational SAR/DSAR process is set out in the separate Subject Access Request (SAR/DSAR) Policy and Procedure (HR-POL-006-06).

11. Data handling, access and confidentiality

- Access personal data only where required for an authorised business purpose.
- Apply least-privilege access and role-based access controls.
- Keep HR, payroll, medical, investigation and legal records confidential and separate where appropriate.
- Do not store Company personal data in unauthorised personal accounts, personal devices, USB drives or unapproved cloud services.
- Use secure sharing methods for payroll, right to work, medical, disciplinary, grievance, legal and commercial records.
- Check recipients carefully before sending personal data by email.
- Report misdirected emails, lost devices, unauthorised access, suspected cyber incidents or suspected breaches immediately.

12. Cyber security and Cyber Essentials Plus

Statom uses layered administrative, physical and technical controls to protect systems and data. Cyber Essentials Plus certification evidences implementation of recognised controls against common cyber threats, but it does not replace UK GDPR accountability obligations.

Control area	Requirement
Firewalls and network controls	Centrally managed, reviewed and monitored.
Secure configuration	Auto-lock, secure default settings, removal of unnecessary accounts and services.
Access control	Role-based access, least privilege, joiner/mover/leaver controls and periodic access reviews.
Malware protection	Endpoint protection, monitoring and prompt response to alerts.
Software updates	Patching in line with risk, vendor guidance and operational priority.
Backups and recovery	Appropriate backup, restoration and resilience measures for business-critical systems.
Incident response	Defined escalation, investigation, containment, recovery and reporting process.

13. Personal data breaches and security incident response

A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A security incident may also involve systems, devices, networks, confidential information or business-critical information, even where it is not yet clear whether personal data is affected.

13.1 Immediate reporting

All employees, workers, contractors, managers and third parties working on behalf of Statom must report any actual or suspected personal data breach or security incident immediately and, wherever possible, no later than the same working day. Reports must be made to IT and the Data Protection Lead. Where the incident involves HR, payroll, health, occupational health, disciplinary, grievance, right to work, site access or employee records, HR must also be informed.

Individuals must not investigate alone, delay reporting, delete evidence, alter records, forward affected data unnecessarily or attempt to conceal the incident.

13.2 Examples of reportable incidents

- email or documents sent to the wrong recipient;
- lost or stolen laptop, phone, memory stick, paper file, ID document or payroll record;

- unauthorised access to HR, payroll, site, CCTV, medical or employee records;
- ransomware, malware, phishing compromise, account takeover or suspected system intrusion;
- loss, corruption or accidental deletion of personal data;
- disclosure of health, absence, disciplinary, grievance, pay or right to work information to someone without authority;
- supplier, payroll, benefits, occupational health, recruitment or IT provider incident affecting Statom data.

13.3 Breach response steps

- Contain the incident immediately, including recalling emails, disabling access, isolating devices, securing files and preserving evidence where appropriate.
- Record when the incident was discovered and when Statom became aware of facts indicating that a personal data breach may have occurred.
- Assess what happened, what data is affected, who is affected, whether the data is protected, and the likely risk to individuals.
- Decide whether the incident is reportable to the ICO within 72 hours of becoming aware, where feasible, and document the reasoning even where the decision is not to report.
- Decide whether affected individuals must be informed without undue delay because the breach is likely to result in a high risk to their rights and freedoms.
- Complete corrective actions, review root cause, record lessons learned and track actions to completion.

13.4 Breach assessment and record keeping

The Data Protection Lead, with support from IT, HR, Legal, Payroll and relevant managers where required, will assess and record:

- the date and time the incident was identified and reported;
- the date and time Statom became aware of the breach;
- the nature and cause of the incident;
- the personal data involved and whether special category or criminal offence data is affected;
- the individuals affected and approximate number of records involved;
- the likely consequences and level of risk for individuals;
- containment, recovery and mitigation action taken;
- whether the breach is reportable to the ICO and the reasons for the decision;
- whether affected individuals must be informed and the reasons for the decision;
- lessons learned, corrective actions, action owners and completion dates.

All breaches, suspected breaches and near misses must be recorded in the Company breach register, including incidents that are not reported to the ICO. Records must be sufficiently detailed to demonstrate accountability, investigation steps, risk assessment, notification decisions, containment action and lessons learned.

13.5 Notification to the ICO and affected individuals

Where legally required, the Company will notify the ICO within 72 hours of becoming aware of a reportable personal data breach, where feasible. If notification is made later than 72 hours, the reason for the delay must be recorded.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, the Company will inform affected individuals without undue delay. Communications must be clear, accurate and coordinated by the Data Protection Lead, with support from HR, IT, Legal, Payroll, insurers and senior management where appropriate.

14. Data protection complaints procedure

Individuals may make a data protection complaint if they are concerned about how Statom has collected, used, stored, shared, retained, deleted or otherwise handled their personal data.

- Complaints may be submitted verbally or in writing to the Data Protection Lead, Chief People Officer, HR, IT or the relevant manager.
- The recipient must forward the complaint to the Data Protection Lead without delay.
- Statom will acknowledge the complaint without undue delay and in any event within 30 days, explain the process and request any information reasonably needed to investigate it.
- Statom will investigate fairly and proportionately, involving HR, IT, Legal, Payroll or managers only where necessary.

- Statom will investigate and provide an outcome in writing without undue delay. Where the investigation cannot reasonably be completed promptly, Statom will keep the complainant informed of progress and the expected timescale.
- The outcome will explain what has been found, any action taken or proposed, and the individual's right to raise the matter with the ICO if they remain dissatisfied.

Complaints must not result in retaliation, victimisation or detrimental treatment. Managers must escalate complaints and must not attempt to suppress, delete or alter relevant records.

15. Retention and disposal

Personal data must not be kept longer than necessary. Retention must reflect legal limitation periods, statutory obligations, operational need, regulatory expectations, insurance requirements and the likelihood of claims.

Record type	Indicative retention approach
Recruitment records for unsuccessful applicants	Normally 6 to 12 months after recruitment outcome, unless longer retention is justified.
Right to work checks	Duration of employment plus at least 2 years.
Payroll, tax and pension records	Normally 6 years plus current year, or longer where required by law or audit.
Personnel file and contract records	Duration of employment plus up to 6 years, unless a longer period is justified.
Working time, holiday and absence records	In line with statutory requirements and limitation periods; normally up to 6 years where needed for claims or audit.
Disciplinary, grievance and investigation records	Retained according to seriousness, outcome, legal risk and proportionality; normally up to 6 years unless longer is justified.
Health, occupational health and medical records	Retained only for as long as necessary for employment, health and safety, legal, insurance or occupational health purposes.
Accident, health and safety, exposure or site incident records	In line with statutory, insurance, limitation and sector requirements. Some records may need longer retention.
CCTV and access control records	Normally short retention unless needed for investigation, legal, security, safety or insurance purposes.
Supplier, client and contract records	Duration of relationship plus relevant limitation, tax, audit and contract periods.
Breach register and breach investigation records	Retained for accountability, regulatory, legal and audit purposes, normally up to 6 years unless a longer period is justified.

A detailed retention schedule should be maintained separately and reviewed annually. Secure deletion, anonymisation, return or destruction must be used when retention ends.

16. International transfers and processors

Statom will not transfer personal data outside the UK unless the transfer is lawful and protected by appropriate safeguards. This includes checking cloud, HR, payroll, recruitment, benefits, IT support, email, backup, collaboration and cyber security systems.

- UK adequacy regulations where available;
- the UK International Data Transfer Agreement or UK Addendum to EU Standard Contractual Clauses where required;
- transfer risk assessments where required;
- processor contracts with clear instructions, confidentiality, security, sub-processor, audit, assistance and return/deletion obligations.

17. Monitoring, CCTV, email, internet and devices

Statom may monitor Company systems, devices, networks, premises, sites, vehicles and equipment where lawful, necessary and proportionate for business, security, safety, compliance, quality, investigation or legal purposes.

Monitoring must have a lawful basis and be explained in the relevant privacy notice, CCTV notice, vehicle notice, IT notice or local notice unless an exemption applies. Covert monitoring will only be used in exceptional circumstances, where justified, authorised and legally compliant.

Managers must not introduce new monitoring technologies or practices without HR, IT and Data Protection Lead approval.

18. Automated decision-making, profiling and AI tools

Statom will only use solely automated decision-making that produces legal or similarly significant effects where a valid lawful basis and the statutory conditions are satisfied. Appropriate safeguards will include transparency, the opportunity for the individual to make representations, obtain human intervention and contest the decision. Significant automated decisions involving special category data will be subject to the additional statutory restrictions and safeguards.

AI-enabled tools must not be introduced for HR, recruitment, payroll, monitoring, selection, performance, absence management or disciplinary purposes without prior assessment of lawful basis, fairness, bias risk, transparency, security, supplier controls, human oversight and privacy information.

19. Training and awareness

- Employees, workers and relevant contractors must complete data protection and cyber security training at induction and at appropriate intervals afterwards.
- Managers, HR, Payroll, IT and anyone handling sensitive records may receive additional role-specific training.
- Training records must be retained and monitored for completion.
- Failure to complete required training may be escalated to management and may be treated as a conduct issue where appropriate.

20. Roles and responsibilities

Role	Responsibility
Board / Senior Management	Policy approval, governance, resourcing and accountability.
Chief People Officer / Data Protection Lead	Data protection governance, privacy notices, rights requests, complaints, breach coordination, HR compliance and training oversight.
Head of IT / IT Systems Manager	Cyber security, patching, access control, technical controls, asset reviews, incident response and audit readiness.
Managers	Apply this policy, minimise data collection, protect team records, escalate requests, complaints and breaches, and consult before new processing.
Employees, workers and contractors	Follow this policy, protect data, use approved systems, complete training and report incidents immediately.
Processors and suppliers	Process personal data only under written contract and documented instructions.

21. Non-compliance

Failure to comply with this policy may result in disciplinary action, termination of engagement, contractual remedies, reporting to regulators, legal claims, suspension of system access or other action depending on the seriousness of the breach.

22. Review and updates

This policy will be reviewed annually or earlier following legal, regulatory, operational, system, supplier, cyber security or risk changes. Material changes will be communicated to staff, contractors and relevant third parties.

Appendix 1 - Employee, Worker and Contractor Privacy Notice

Purpose of this notice

This privacy notice explains how Statom uses personal data about employees, workers, apprentices, CIS contractors, agency workers, consultants and other individuals engaged to work for or on behalf of the Company. It does not form part of any contract of employment or engagement.

Who controls your personal data?

Statom is the controller for most employment and engagement-related personal data. Some group companies may also act as controller where they determine the purpose and means of processing.

What personal data do we collect?

- identity, contact and emergency contact details;
- employment, engagement, payroll, pension, tax, benefits, expenses and bank details;
- right to work, qualification, licence, training, competence and certification records;
- absence, health, occupational health, reasonable adjustment and medical information;
- performance, appraisal, promotion, disciplinary, grievance, investigation and exit records;
- IT, device, email, access, CCTV, site, vehicle, plant and telematics information where relevant;
- equal opportunity monitoring information where collected.

Why do we use it?

- to administer employment, engagement, pay, tax, pension, benefits and expenses;
- to manage work allocation, site access, competence, safety, training, attendance and performance;
- to meet legal obligations, including employment, tax, immigration, health and safety and equality obligations;
- to manage absence, occupational health, wellbeing, reasonable adjustments and fitness for work;
- to protect Company systems, people, premises, assets and confidential information;
- to investigate concerns, manage disputes, defend legal claims and support audits;
- to support workforce planning, reporting, succession, engagement and business operations.

Lawful basis and special category conditions

We rely on contract, legal obligation, legitimate interests, vital interests in emergencies and, rarely, consent. For special category data, we rely on employment law obligations, occupational health or working capacity, substantial public interest, legal claims, vital interests or explicit consent where appropriate. Consent will not usually be relied on where another lawful basis is more appropriate in an employment context.

Who do we share it with?

- HMRC, pension providers, benefit providers, payroll providers, auditors, insurers and professional advisers;
- occupational health providers, medical advisers and health and safety advisers where needed;
- clients, principal contractors, site operators, accreditation bodies or training providers where required for site access, competence or contractual compliance;
- IT, HR, payroll, recruitment, document management, cloud, cyber security and communication service providers;
- regulators, law enforcement, courts, tribunals or public authorities where required or permitted by law.

How long do we keep it?

We keep personal data only for as long as necessary for the purpose collected, including legal, statutory, insurance, audit and claim periods. Indicative retention periods are set out in section 15 and the detailed retention schedule.

Your rights, questions and complaints

You have rights to be informed, access your data, rectify inaccuracies, request erasure or restriction, object, request portability, and challenge certain automated decisions. These rights are subject to legal limits and exemptions. You can raise questions, rights requests or complaints with the Data Protection Lead, Chief People Officer, HR or your manager. You also have the right to complain to the ICO.

Appendix 2 - Recruitment Applicant Privacy Notice

This notice applies to job applicants, candidates, work experience applicants and individuals considered for employment or engagement by Statom.

What we collect

- name, contact details, CV, application information and employment history;
- interview notes, assessment results, right to work information, qualifications and references;
- equal opportunity monitoring information where collected;
- health or reasonable adjustment information where needed for recruitment or assessment;
- background, licence, site access or vetting information where relevant to the role and legally permitted.

Why we use it

- to assess suitability for the role or opportunity;
- to communicate with candidates and arrange interviews or assessments;
- to complete pre-employment checks and right to work checks;
- to make recruitment decisions and manage offers;
- to meet legal obligations and defend legal claims.

Lawful basis, sharing and retention

We rely on legitimate interests, steps before entering into a contract, legal obligation and, where appropriate, consent. Special category data is processed only where a lawful Article 9 condition applies, for example employment law obligations, substantial public interest, reasonable adjustments, legal claims or explicit consent where appropriate.

We may share applicant data with recruitment agencies, assessment providers, background check providers, referees, IT providers, professional advisers and regulators where needed. Unsuccessful applicant records are normally retained for 6 to 12 months unless longer retention is justified, for example for talent pooling with consent or for legal claims.

Automated decision-making

Statom will not make significant recruitment decisions based solely on automated processing unless a valid lawful basis and statutory conditions apply and appropriate safeguards are in place, including transparency, representations, human intervention and the ability to contest the decision.

Appendix 3 - Supplier, Subcontractor, Client and Visitor Privacy Notice

This notice applies to supplier contacts, subcontractor contacts, client contacts, visitors, site contacts, professional advisers and other third-party business contacts.

What we collect

- business contact details, role, organisation and communication records;
- contract, procurement, account, payment and due diligence records;
- site access, identity, competence, training, health and safety and induction records where relevant;
- CCTV, premises access, vehicle, plant or site security information where used;
- insurance, accreditation, licence, compliance and audit information.

Why we use it

- to manage contracts, procurement, projects, payments and business relationships;
- to control site and premises access and meet health and safety obligations;
- to protect people, assets, systems and confidential information;
- to manage disputes, audits, insurance, legal claims and regulatory requirements.

Lawful basis, sharing, retention and rights

We rely on contract, legal obligation and legitimate interests. We may share data with group companies, clients, principal contractors, site operators, insurers, auditors, professional advisers, regulators, law enforcement, IT providers and other service providers where necessary and lawful.

We retain third-party data for as long as necessary for the relationship, contract, project, audit, legal, insurance and regulatory purposes. Individuals have the rights set out in section 10, subject to legal limits and exemptions.

Appendix 4 - Website, Cookies and Electronic Communications Notice

Where Statom websites use cookies, analytics, tracking technologies, online forms or electronic marketing, a website privacy notice and cookie notice must explain what is used, why, how long it lasts, who receives the data and how users can manage consent or preferences.

- Strictly necessary cookies may be used without consent where they are essential to provide the requested service.
- Analytics, advertising, tracking or non-essential cookies must not be set unless valid consent has been obtained where required by PECR.
- Marketing emails, SMS or similar electronic communications must comply with PECR and UK GDPR.

Appendix 5 - Quick Reporting Guide

Issue	What to do immediately
Lost device, misdirected email, unauthorised disclosure or suspected cyber incident	Report immediately to IT and the Data Protection Lead. Do not delay while investigating alone. Preserve evidence.
Data subject access request or other rights request	Forward immediately to the Data Protection Lead/HR. Requests can be verbal or written.
Data protection complaint	Acknowledge receipt where appropriate and forward to the Data Protection Lead without delay.
New system, supplier, monitoring tool, AI tool or data collection process	Do not proceed until HR, IT and Data Protection Lead review is complete.
Request to share health, absence, disciplinary, payroll or right to work information	Check authority and lawful basis before sharing. Escalate to HR/Data Protection Lead if unsure.

Appendix 6 - Data Breach Response Report Form and Assessment Checklist

This form/checklist should be completed by the Data Protection Lead or delegated incident lead. It may be held electronically in the breach register. It should be started as soon as a suspected incident is reported and updated as facts are confirmed.

Assessment point	Record details
Incident reference	
Reported by / team / contact details	
Date and time discovered	
Date and time reported to Statom	
Date and time Statom became aware of the breach	
Systems, files, locations, devices or suppliers involved	
Description of incident	
Type of personal data involved	
Special category or criminal offence data involved?	
Approximate number of individuals affected	
Categories of individuals affected	Employees / workers / contractors / applicants / clients / suppliers / visitors / other
Containment action taken	
Is the data encrypted, password protected or otherwise secured?	
Likely consequences for individuals	

Risk level	Low / medium / high - include reasons
ICO notification required?	Yes / no - include reasons
Affected individuals to be informed?	Yes / no - include reasons
External support required?	Legal / insurer / cyber specialist / police / supplier / other
Corrective actions, owners and deadlines	
Closure date and lessons learned	

Appendix 7 - Data Subject Rights Request Handling Guide

1. Forward all rights requests to the Data Protection Lead/HR immediately. Requests may be verbal or written and do not need to mention UK GDPR.
2. Verify the requester's identity where appropriate before disclosing personal data.
3. Clarify the request where reasonably needed and permitted by law.
4. Identify relevant systems, files, emails and records using reasonable and proportionate searches.
5. Review the data for third-party information, legal privilege, management forecasting, confidential references, crime and taxation exemptions, negotiations, or other applicable exemptions.
6. Provide the response without undue delay and normally within one calendar month, unless a lawful extension applies.
7. Keep a record of the request, search steps, decisions, exemptions and response.

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.*