Data Protection Policy

STATEMENT OF GENERAL INTENT

Introduction

Strategy IT Limited is committed to protecting the rights and privacy of individuals whose personal data we process. We gather and use personal information relating to employees, customers, suppliers, business contacts and other parties with whom we have a business relationship. We will ensure compliance with the UK GDPR, the Data Protection Act 2018 and relevant ICO Guidance & Codes of Practice.

Purpose

- Protect individuals' rights.
- Provide clear responsibilities and demonstrate accountability.
- Promote transparency, integrity and wellbeing.
- Ensure compliance with UK law and ethical business practice.

Scope

- All employees, temporary staff, contractors, suppliers and third parties handling personal data on behalf of Strategy IT Limited.
- All personal data processed in electronic or paper formats.
- Personal data relating to employees, clients, suppliers and partners.

Legal & Regulatory Alignment

Legislation / Regulation	Key Focus
UK GDPR	Lawful, fair, transparent and secure handling of personal data, covering principles of processing, lawful bases, data subject rights and accountability.
Data Protection Act 2018	UK-specific provisions, exemptions and enforcement mechanisms supplementing UK GDPR.
Privacy and Electronic Communications Regulations (PECR)	Rules on electronic marketing, cookies and communications, consent requirements and restrictions on unsolicited marketing.
ICO Guidance and Codes of Practice	Includes statutory Data Sharing Code of Practice, Direct Marketing Code and other guidance to support compliance with UK GDPR & PECR.

RESPONSIBILITIES

Role	Key Responsibility
Employees	Comply with this policy and complete training. Maintain confidentiality of personal data. Promptly report suspected or actual breaches. Cooperate with audits, compliance checks and investigations.
Suppliers / Contractors / Third Parties (processing personal data on behalf of Strategy IT)	Uphold this policy and comply with all applicable UK law. Maintain confidentiality of personal data and implement appropriate security measures. Seek approval before using sub-processors and return/delete data at contract end. Promptly report breaches. Cooperate with audits, compliance checks and investigations.
Data Protection Lead	Act as the point of contact for data subjects and the ICO. Oversee training, compliance, monitoring and reporting. Coordinate and conduct breach investigation. (Note: Strategy IT Limited is not legally required to appoint a Data Protection Officer under UK GDPR (Article 37), as our core activities do not involve large-scale monitoring or large-scale processing of special category data.)
Directors	Lead by example, ensure staff awareness, act promptly and appropriately on breaches. Maintain accountability and oversight.
Company	Provide training, guidance, resources, secure systems, fair and transparent monitoring.

ARRANGEMENTS

1. Definitions

- **Personal Data**: Information relating to an identifiable individual
- **Special Category Data**: Sensitive data (e.g. health, racial/ethnic origin)
- **Data Subject**: The individual to whom personal data relates
- **Controller**: Strategy IT Limited
- **Processor**: Third parties processing data on behalf of Strategy IT Limited
- **Processing**: Any operation performed on personal data (e.g. collection, recording, storage, use, disclosure, deletion)

2. Data Protection Principles

We commit to the principles in UK GDPR (Article 5):

- **Lawfulness, Fairness & Transparency** – Personal data is processed lawfully, fairly, and transparently.
- **Purpose Limitation** – Data is collected only for specified, legitimate purposes.
- **Data Minimisation** – Data is adequate, relevant, and limited to what is necessary.
- **Accuracy** – Data is accurate and kept up to date.
- **Storage Limitation** – Data is retained only for as long as necessary. Strategy IT Limited retains personal data only for defined periods in line with legal and business requirements as detailed in the Retention Data Schedule (Appendix 1), after which data is securely deleted or anonymised.
- **Integrity & Confidentiality** – Data is kept secure using appropriate technical and organisational measures.
- **Accountability** – Accountability is demonstrated through documented compliance measures.

3. **Lawful Bases for Processing**

   Processing will only occur under one of the following lawful bases in UK GDPR (Article 6):

   - **Consent** – The individual has clearly agreed to the use of their data for a specific purpose.
   - **Contract** – Data is needed to deliver a contract or take steps before entering into one.
   - **Legal Obligation** – Data must be processed to comply with UK law (e.g. tax or employment law).
   - **Vital Interests** – Data is processed to protect someone's life or safety.
   - **Legitimate Interests** – Data is used for a genuine business reason, balanced against the individual's rights and freedoms.
   - **Public Task** (where applicable) – Data is processed to carry out official functions or tasks in the public interest, where legally authorised.

4. **Data Subject Rights**

   Individuals (Data Subjects) have the right to:

   - **Be Informed** – People must be told how their data is collected, used and shared.
   - **Access (Subject Access Requests)** – People can request a copy of the personal data we hold about them. Subject Access Requests (SARs) must be responded to within one calendar month, extendable to two months if complex.
   - **Rectification** – People can ask for incorrect or incomplete data to be corrected.
   - **Erasure (The Right to be Forgotten)** – People can request deletion of their data when there is no legal reason to keep it.
   - **Restriction of Processing** – People can ask us to limit how their data is used in certain circumstances.
   - **Data Portability** – People can request their data in a usable format or ask for it to be transferred to another organisation.
   - **Objection** – People can object to their data being used for certain purposes, such as marketing.
   - **Challenge Automated Decision Making** – People can challenge decisions made solely by automated systems without human involvement.

5. **Data Sharing & Transfers**

   - Data shared only with authorised third parties under written agreements.
   - All suppliers and processors handling personal data on behalf of Strategy IT Limited must have a Data Processing Agreement (DPA) in place.
   - Transfers of personal data outside the UK will only occur in compliance with UK adequacy regulations, the International Data Transfer Agreement (IDTA), or other approved safeguards.

6. **Marketing & Communications**

   - Compliance with PECR for email, SMS and phone marketing.
   - Cookies and tracking technologies used only with clear consent.

7. **Security Measures**

   - Paper records stored securely.
   - Electronic records protected by encryption, firewalls and MFA.
   - Regular backups and secure server locations.
   - Removable media encrypted and locked away.
   - Access restricted to authorised staff only.
   - Compliance with Acceptable Use Policy.

8. **Incident Reporting & Breach Management**
    - All incidents must be reported immediately to the Board of Directors.
    - Data breaches must be escalated to the Data Protection Lead within 24 hours (the company is not legally required to appoint a DPO and instead has a Data Protection Lead).
    - Information Commissioner's Office (ICO) notification will be made within 72 hours where required:
        Helpline: 0303 123 1113
        Website: ico.org.uk
        Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
    - If a data breach could put individuals at high risk, Strategy IT Limited will inform them without undue delay and provide clear information about the nature of the breach, its impact and mitigation measures (UK GDPR Article 34).
    - Breach log maintained for accountability.
    - Business continuity and disaster recovery procedures will be followed.

9. **Monitoring & Accountability**
    - Processing activities records required under UK GDPR (Article 30):
        - Controller/Processor details – names, contact info
        - Purposes of processing – why the data is being used
        - Categories of data subjects – e.g. employees, clients, suppliers
        - Categories of personal data – e.g. contact details, financial, health
        - Recipients of data – who data is shared with
        - International transfers – details of transfers outside the UK and safeguards used
        - Retention schedules – how long data is kept before deletion/anonymisation
        - Security measures – description of technical and organisational protections
    - Lawful basis assessments
    - Training logs
    - Data subject rights requests
    - Breach logs

10. **Training & Awareness**
    - Induction training provided to all new staff.
    - Mandatory annual refresher training provided on handling personal data, confidentiality and breach reporting.
    - Policies and guidance (e.g. plain-language summaries, infographics) are issued to all employees during induction, available on the company intranet and notice boards, reviewed annually and updated as required.

11. **Whistleblowing & Reporting Concerns**
    - Concerns can be reported to any member of the Board.
    - Anonymous reporting permitted.
    - Reports investigated fairly, promptly and confidentially.

- Retaliation against whistleblowers will not be tolerated, in line with the Public Interest Disclosure Act 1998 and the whistleblowing protections within the Employment Rights Act (as amended by the Employment Rights Act 2025, including sexual-harassment-related disclosures).

12. Disciplinary Consequences

- Breaches may result in disciplinary action, up to and including dismissal, in line with the Disciplinary, Dismissal & Grievance Policy.
- Serious breaches may be reported to regulators or law enforcement.

13. Review

- This policy will be reviewed annually (or sooner if legislation changes) to ensure effectiveness, compliance with UK law and alignment with best practice.
- Updates will be communicated to all staff.

Approved by: Board of Directors, Strategy IT Limited
Date: 01/04/2026

Retention Data Schedule (Appendix 1)

Strategy IT Limited retains personal data only for defined periods in line with legal and business requirements as detailed in the, after which data is securely deleted or anonymised.

Data Type	Retention Period	Legal / Business Basis
Recruitment Records (unsuccessful candidates)	6 months from the conclusion of the recruitment process	ICO guidance (fairness and data minimisation)
HR & Employee Records	6 years after employment ends	Limitation Act 1980 (employment claims)
Training Records (e.g. induction, annual refresher & mandatory modules)	6 years after employment ends	Evidence for tribunal or ICO investigations; UK GDPR (accountability); Limitation Act 1980
Disciplinary, Dismissal & Grievance Procedure Records	6 years after employment ends	UK GDPR & Data Protection Act 2018 (legal obligation and legitimate interests)
Whistleblowing Reports & Investigation Records	6 years after the investigation is closed	Public Interest Disclosure Act 1998; Employment Rights Act 1996; Limitation Act 1980
Confidentiality Agreements / NDAs	6 years after the agreement expires or is terminated	Limitation Act 1980 (contract claims)
Payroll & Tax Records	7 years	HMRC requirements
Financial Accounts & Invoices	7 years	HMRC requirements
Client Contracts & Project Files	6 years after the contract ends	Limitation Act 1980 (contract claims)
Supplier Due Diligence Records (e.g. Modern Slavery checks & security vetting)	6 years after the supplier relationship ends	Modern Slavery Act 2015; UK GDPR (accountability); Limitation Act 1980
Business Continuity & Disaster Recovery Records	6 years	UK GDPR (accountability); audit and insurance requirements
Health & Safety Records	3 years (or longer where required by specific regulations)	Health and Safety legislation
Risk Assessments (e.g. H&S, DSE, fire & remote working)	6 years	MHSWR 1999; HSWA 1974; Limitation Act 1980
IT Security Logs (e.g. access logs, VPN logs, firewall logs & authentication logs)	6–24 months depending on system type and security requirements	UK GDPR (security and accountability); Cyber Essentials; legitimate interests
Security Camera Footage	Up to 60 days (subject to system configuration and proportionality assessment)	UK GDPR (data minimisation and security); legitimate interests (crime prevention and safety)
Marketing Data (consent-based)	Until consent is withdrawn or after 2 years of inactivity	UK GDPR (consent requirements)
Website Cookies & Tracking Data	Session cookies deleted on browser close; persistent cookies retained for up to 12 months unless consent is withdrawn	PECR & UK GDPR (consent, transparency and minimisation)
Subject Access Requests	3 years after the request is closed	UK GDPR (accountability); ICO guidance