Data Protection Policy

Strategic Data Consultancy Ltd

Document Ref: SDC-POL-DP-001
Version: 1.0 – Initial Version
Date: 12 April 2026
Review Date: 11 April 2027

---

1. Purpose

This policy sets out how Strategic Data Consultancy Ltd (SDC) protects personal data and ensures it is handled in a lawful, fair, and transparent manner in accordance with the UK GDPR and the Data Protection Act 2018.

SDC recognises the importance of maintaining the confidentiality, integrity, and availability of personal data in the delivery of its services.

In addition to personal data, SDC recognises that it handles commercially sensitive client data, including survey and asset information. Such data is managed in accordance with client-specific requirements and contractual obligations, and is handled with appropriate controls to ensure its security, integrity, and confidentiality.

---

2. Scope

This policy applies to all personal data processed by SDC in the course of its business activities, including:

- Client and stakeholder contact details
- Supplier and subcontractor information
- Employee data (where applicable)
- Data captured during site surveys where individuals may be identifiable

---

3. Responsibility

Given the size and structure of the business, overall responsibility for data protection sits with:

John Sutherns – Director

The Director will:

- Ensure compliance with applicable data protection legislation
- Determine the purposes and lawful basis for processing data
- Ensure appropriate technical and organisational measures are in place
- Respond to data protection queries or incidents
- Maintain awareness of data protection responsibilities

4. Data Protection Principles

SDC will ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as necessary
- Processed securely to prevent unauthorised access, loss, or damage

5. Lawful Basis for Processing

SDC processes personal data under the following lawful bases:

- Contractual necessity – to deliver services to clients
- Legitimate interests – for business development, communication, and operational management
- Legal obligation – where required for compliance with legal or regulatory requirements

6. Data Collection and Use

SDC will only collect personal data where necessary and relevant to its operations.

Typical uses include:

- Managing client relationships and project delivery
- Communicating with clients, suppliers, and stakeholders
- Producing reports, asset registers, and supporting documentation
- Maintaining business records and accounts

Where survey data may include identifiable individuals, reasonable steps will be taken to minimise or avoid capturing personal data.

7. Data Storage and Security

SDC uses secure digital systems to store and manage data, including:

- Microsoft 365 (OneDrive, SharePoint, Outlook)
- Xero (financial records)
- Expensify (expenses and receipts)

Security measures include:

- Password-protected devices and accounts
- Multi-factor authentication where available
- Restricted access to data
- Regular software updates and security patches

Data will not be stored on unsecured devices or shared without appropriate safeguards.

8. Data Sharing

SDC may share personal data with:

- Clients and project stakeholders
- Professional advisers (e.g. accountants)
- Software providers and cloud services

Data will only be shared where necessary and appropriate safeguards are in place.

SDC does not sell personal data to third parties.

---

9. Data Retention

Personal data will be retained only for as long as necessary to fulfil its purpose.

Typical retention includes:

- Project records – retained for contractual and audit purposes
- Financial records – retained in line with statutory requirements

Data will be securely deleted or anonymised when no longer required.

---

10. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request erasure where applicable
- Object to or restrict processing
- Lodge a complaint with the Information Commissioner's Office

Requests will be responded to within one month where applicable.

---

11. Data Breaches

In the event of a data breach, SDC will:

- Assess the nature and impact of the breach
- Take immediate steps to contain and mitigate risks
- Notify affected parties where required
- Report to the Information Commissioner's Office where legally required

---

12. Monitoring and Review

This policy will be reviewed annually or in response to:

- Changes in legislation
- Changes in business operations
- Identified risks or incidents

---

13. Commitment

SDC is committed to ensuring that personal data is handled responsibly and securely as part of its overall professional and ethical standards.

Signed:
John Sutherns
Director