PROTECTION & PRIVACY POLICY

1. About This Policy

Shelton Development Services Ltd ("SDS", "we", "us", "our") is committed to protecting the privacy and security of personal data. This policy explains how we collect, use, store, share, and protect personal data, and sets out the rights of individuals whose data we process.

This policy applies to:

- Customers, prospects, and their employees who interact with SDS products and services.
- SDS employees and contractors.
- Job applicants and candidates.
- Website visitors and users of SDS digital platforms.
- Suppliers, partners, and third parties whose data SDS holds.

SDS is a data controller under UK GDPR for personal data it collects directly. Where SDS processes personal data on behalf of clients, SDS acts as a data processor operating under the client's instructions. This policy covers both roles.

Legal Framework
This policy is aligned with:
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025 (DUAA 2025) — amending UK GDPR from August 2025
- Privacy and Electronic Communications Regulations 2003 (PECR)
- ISO/IEC 27001:2022 Annex A Control A.5.34 – Privacy and Protection of PII

2. Our Data Protection Principles

SDS processes personal data in accordance with the seven principles of UK GDPR (Article 5). We will:

- **Lawfulness, Fairness & Transparency:** Process personal data lawfully, fairly and transparently. We will always tell you what data we hold and why.
- **Purpose Limitation:** Collect data for specified, explicit, and legitimate purposes only. We will not use it for incompatible purposes.
- **Data Minimisation:** Collect only what is necessary. We will not gather more personal data than we need.
- **Accuracy:** Keep personal data accurate and up to date. We will take reasonable steps to correct inaccuracies.
- **Storage Limitation:** Keep personal data only for as long as necessary. We will delete or anonymise data when it is no longer needed.
- **Integrity & Confidentiality:** Protect personal data using appropriate technical and organisational security measures.
- **Accountability:** Demonstrate compliance with these principles. We maintain a Record of Processing Activities (ROPA) and appoint a qualified DPO.

3. What Personal Data We Collect and Why

3.1 Customers, Prospects and Client Contacts

When you engage with SDS as a customer, prospect, or client contact, we collect:

- Name, job title, company name, and professional contact details (email, phone, address).
- Communications history (emails, support tickets, meeting notes).
- Contract and purchasing information.
- Usage data relating to SDS-hosted products and services.

We use this data to: deliver contracted products and services; manage the commercial relationship; provide technical support; send relevant product and service communications; and meet legal and contractual obligations.

3.2 Client Employees (where SDS processes data as a processor)

Where SDS processes personal data on behalf of its clients (for example, employee data held within SDS-hosted products), we act as a data processor operating under the client's instructions as set out in the relevant contract and data processing agreement. In this role, we only process data for the purposes the client directs and do not use it for SDS's own purposes.

3.3 SDS Employees and Contractors

We collect and process personal data about our employees and contractors throughout the employment lifecycle, including:

- Identification and contact information (name, address, National Insurance number, date of birth).
- Employment records (contracts, payroll, salary, bank details, tax information).
- Right to work documentation.
- Performance and training records.
- Absence and health data (limited; special category).
- IT system access records and audit logs.

This data is processed to fulfil our legal obligations as an employer and to manage the employment relationship. Full details are set out in our Employee Privacy Notice provided at onboarding.

3.4 Job Applicants

When you apply for a role at SDS, we collect: name, contact details, CV and application information, interview notes, and pre-employment screening results (where applicable). We retain unsuccessful candidate data for up to 12 months unless a longer period is justified. We will ask for your permission before retaining your data beyond this period for future opportunities.

3.5 Website Visitors

When you visit www.s-d-s.co.uk, we may automatically collect: IP address, browser type and version, pages visited, referring website, timestamps, and cookie/tracking data. See Section 11 for our full cookie policy. Where you submit a contact form or request, we collect the information you provide.

4. Lawful Basis for Processing

Every processing activity requires a lawful basis under UK GDPR. The table below summarises the bases we rely on and when:

Lawful Basis	When We Use It	Examples
Contract	Processing is necessary to perform a contract with you or take pre-contractual steps	Service delivery, payroll, invoicing
Legal Obligation	Processing is necessary to comply with a legal obligation	PAYE/HMRC reporting, right to work checks, statutory records
Legitimate Interests	Processing is necessary for our legitimate interests, provided these are not overridden by your rights	CRM management, security monitoring, fraud prevention, direct marketing to existing clients
Consent	You have freely given specific, informed consent	Marketing emails to prospects; non-essential cookies
Recognised Legitimate Interests (DUAA 2025)	New statutory category under DUAA 2025 — no balancing test required	Cybersecurity activities, crime prevention, safeguarding

Special Category Data

Some data is treated with extra protection under UK GDPR — this is called "special category data" and includes:

- Health and medical information • Racial or ethnic origin • Religious or philosophical beliefs
- Trade union membership • Biometric or genetic data • Sexual orientation

SDS only processes special category data where: (a) we have explicit consent; (b) processing is necessary for employment law obligations; or (c) another Schedule 1 condition under DPA 2018 applies.
Criminal conviction data is processed only where strictly necessary and permitted by law.

5. How We Use Personal Data

- **Service Delivery:** To provide, maintain, and improve our products and services under contract.
- **Account Management:** To manage client relationships, process payments, and communicate about services.
- **Technical Support:** To diagnose and resolve technical issues raised by clients and their users.
- **Security & Fraud Prevention:** To monitor, detect, and prevent security incidents, fraud, and unauthorised access to SDS systems.
- **Marketing:** To send relevant product updates and communications. You can opt out at any time (see Section 13).
- **Legal Compliance:** To comply with applicable laws, regulations, court orders, and regulatory obligations.
- **HR & Employment:** To manage employment, payroll, benefits, training, and comply with employment law.
- **Business Analytics:** To analyse usage patterns and business performance — using aggregated or anonymised data wherever possible.
- **Business Transfers:** In the event of a sale, merger, or restructuring, personal data may be transferred as part of that transaction, subject to the same data protection obligations.

We will not sell, rent, or lease your personal data to third parties for their independent marketing or commercial use.

6. Data Sharing & Third-Party Processors (ISO 27001:2022 A.5.19–A.5.22)

We share personal data only where necessary and always with appropriate protections. Personal data may be shared with:

- **Technology and SaaS providers:** Platforms we use to deliver services, including AWS, HubSpot, BambooHR, NetSuite, Nexonia, IRIS, DocuSign, Jira, Clockify, and others. All are subject to data processing agreements.
- **HMRC and regulatory authorities:** Where required by law (e.g. payroll reporting, statutory filings).
- **Auditors and professional advisers:** Under strict confidentiality obligations.
- **Law enforcement:** Where required by law or in connection with legal proceedings.
- **Clients (as data processors):** Where SDS processes client employee data in accordance with client instructions under a data processing agreement.
- **Business transfer parties:** In a sale, merger, or restructuring — personal data may transfer as a business asset, subject to this policy.

All third-party processors are assessed before engagement, required to demonstrate adequate security measures, and subject to a written data processing agreement. SDS does not transfer data to any third party for their own independent use.

7. International Transfers

Some of our third-party processors may process personal data outside the UK. Where this occurs, SDS ensures that appropriate safeguards are in place in accordance with UK GDPR Chapter V and the updated transfer standard under the Data (Use and Access) Act 2025 ("not materially lower" standard):

- UK International Data Transfer Agreements (UK IDTA) or Standard Contractual Clauses (SCCs) with the relevant processor.
- Transfer to a country with a UK adequacy decision (e.g. EU/EEA countries).
- Binding Corporate Rules where applicable.

Our Record of Processing Activities (ROPA) sets out the international transfer mechanism for each processing activity. A summary is available on request from our DPO.

8. Data Retention

We retain personal data only for as long as necessary for the purpose for which it was collected, or as required by law. Our standard retention periods are:

Data Type	Retention Period	Reason
Customer and contact data	Duration of contract + applicable legal period	Contractual / legal obligation
Financial and invoice records	7 years	HMRC / Companies Act
Employee records	Employment duration + statutory periods (minimum 6 years post-employment for most records)	Employment law / HMRC
Payslips / P45 / P60	7 years minimum	HMRC statutory obligation
Expense records	7 years	HMRC / Companies Act
Recruitment records	6–12 months (unsuccessful); longer if legal risk	Limitation periods
Website visitor data / cookies	See cookie policy (Section 11)	PECR / consent
Security and access logs	12 months minimum; 5 years for incident-related logs	ISO 27001:2022 / incident forensics
Marketing contact preferences	Until consent withdrawn or opt-out received	PECR / UK GDPR

On expiry of a retention period, personal data is securely deleted or anonymised in accordance with our Data Retention Schedule.

9. Security Measures (ISO 27001:2022 A.5.34 / Article 32 UK GDPR)

SDS implements appropriate technical and organisational measures to protect personal data from unauthorised access, loss, alteration, disclosure, or destruction. Our key measures include:

- **Access controls:** Role-based access control (RBAC) and multi-factor authentication (MFA) on all systems processing personal data.
- **Encryption in transit:** TLS 1.2 minimum (TLS 1.3 preferred) for all data transmissions.
- **Encryption at rest:** AES-256 encryption on all SDS-managed storage and databases.
- **Endpoint security:** Bitdefender and Kaseya VSA endpoint protection on all managed devices.
- **Secure backups:** Daily and monthly encrypted backups; restoration tested quarterly.
- **Audit logging:** Authentication and access events logged and retained for a minimum of 12 months.
- **Incident management:** A documented Incident Response Plan with ICO notification procedures. Personal data breaches are reported to the ICO within 72 hours where required.
- **Staff training:** All staff receive data protection awareness training at induction and annually.
- **Supplier assessments:** All data processors are assessed for security compliance before engagement.
- **ISO 27001:2022 certification:** SDS operates an ISMS aligned to ISO 27001:2022, with regular internal audits and management review.

Full technical details are maintained in our Architecture Standard and are available to clients subject to appropriate confidentiality arrangements.

10. Your Data Subject Rights

Under UK GDPR, you have the following rights in relation to your personal data. You may exercise these rights by contacting our DPO at dpo@s-d-s.co.uk. We will respond without undue delay and within one calendar month (note: the Data (Use and Access) Act 2025 introduces updated SAR provisions including "stop the clock" provisions and a "reasonable and proportionate" search standard):

Right	What It Means	How to Exercise
Right to be Informed	To know how your data is being used — satisfied by this policy and our Privacy Notices	Read this policy; contact DPO with questions
Right of Access (SAR)	To receive a copy of the personal data we hold about you	Submit a request to dpo@s-d-s.co.uk
Right to Rectification	To correct inaccurate or incomplete personal data	Contact dpo@s-d-s.co.uk
Right to Erasure	To request deletion of your personal data where there is no longer a lawful reason to retain it	Contact dpo@s-d-s.co.uk
Right to Restriction	To request that we limit the processing of your data in certain circumstances	Contact dpo@s-d-s.co.uk
Right to Data Portability	To receive your data in a structured, machine-readable format (applies to consent and contract-based processing)	Contact dpo@s-d-s.co.uk
Right to Object	To object to processing based on legitimate interests or for direct marketing purposes	Contact dpo@s-d-s.co.uk or use opt-out links
Rights re Automated Decisions	Not to be subject to solely automated decisions that significantly affect you (under DUAA 2025, strictest controls apply to special category data)	Contact dpo@s-d-s.co.uk

Client Employees and SDS Products

If you are an employee of an SDS client and your personal data is processed within an SDS-hosted product, SDS acts as a data processor on behalf of your employer.

Please contact your employer in the first instance to exercise your data subject rights. Your employer is the data controller for that processing.

If you are unsure who to contact, we are happy to help direct your request — contact us at dpo@s-d-s.co.uk.

If you are not satisfied with our response, you have the right to lodge a complaint with the UK Information Commissioner's Office (ICO): ico.org.uk | 0303 123 1113.

11. Cookies & Website Technologies

When you visit www.s-d-s.co.uk, we may use cookies and similar technologies to improve your experience and gather analytics data.

Cookie Type	Purpose	Consent Required?
Strictly Necessary	Essential for the website to function (e.g. session management, security)	No — legitimate interest
Performance/Analytics	Understand how visitors use our website (e.g. page views, error reports)	Yes — via cookie banner
Functionality	Remember your preferences and personalise your experience	Yes — via cookie banner
Marketing/Targeting	Deliver relevant advertising and track campaign effectiveness	Yes — explicit consent
Low-risk cookies	Cookies that pose minimal privacy risk — exempted from explicit consent requirement under DUAA 2025 amendments to PECR	No — DUAA 2025 exemption

You can manage your cookie preferences at any time via the cookie settings on our website or by adjusting your browser settings. Note: disabling certain cookies may affect website functionality.

Social media features on our website (e.g. "Like" buttons, share widgets) may collect data such as your IP address and the pages you visit, and may set cookies. Their use is governed by the privacy policy of the relevant social media platform.

12. Employee & Staff Data (Internal)

This section supplements the general policy for SDS employees, contractors, and candidates. A full Employee Privacy Notice is provided at onboarding and is available from HR.

12.1 Monitoring

SDS reserves the right to monitor, filter, and audit activity on SDS systems and networks for the purposes of security, compliance, and operational management. Users of SDS systems should have no expectation of privacy when using SDS resources. Monitoring is conducted in accordance with the Investigatory Powers Act 2016, Employment Rights Act 2025, and the SDS Acceptable Use Policy. Staff are notified of monitoring through this policy and their employment contract.

12.2 Mobile Devices & Remote Working

Mobile devices used to access SDS systems or containing SDS data must be protected by a PIN, password, or biometric authentication. Devices must lock automatically after a maximum of 10 minutes of inactivity. SDS data must not be stored on personal devices without authorisation. Refer to the Acceptable Use Policy for full requirements.

12.3 Training

All staff must complete data protection awareness training at induction and at least annually thereafter. Training completion is recorded as documented evidence by HR. Failure to complete mandatory training will be treated as a policy breach.

12.4 Reporting Concerns

Any suspected data protection breach or mishandling of personal data must be reported immediately to the DPO (dpo@s-d-s.co.uk). SDS prohibits any form of retaliation against staff who report data protection concerns in good faith. Retaliation will be treated as a disciplinary matter.

13. Marketing Communications

Where we send marketing communications, we do so on the basis of your consent (for prospects) or our legitimate interest (for existing clients in respect of related products and services).

You can opt out of marketing communications at any time by:

- Clicking "unsubscribe" in any marketing email.
- Emailing dpo@s-d-s.co.uk with your preference.
- Contacting us at support@s-d-s.co.uk.

Opting out of marketing will not affect the delivery of contracted services or transactional communications.

14. Children's Data

SDS products and services are not directed at children under the age of 18. We do not knowingly collect personal data from children. If we become aware that we have inadvertently collected personal data from a child, we will delete it promptly. If you believe we hold data about a child, please contact dpo@s-d-s.co.uk.

15. Changes to This Policy

We may update this policy from time to time to reflect changes in our practices, the law, or our business. Material changes will be communicated to relevant individuals (for example, by email or website notice). The current version of this policy is always available at www.s-d-s.co.uk. Continued engagement with SDS following a material update constitutes acceptance of the revised policy.

16. Contact Us & Our Data Protection Officer

Data Protection Officer
Nicole Kiezun – Head of Operations & DPO
Email: dpo@s-d-s.co.uk
Post: Shelton Development Services, [Address], United Kingdom
General enquiries: support@s-d-s.co.uk | www.s-d-s.co.uk

To exercise your data subject rights, to report a concern, or to ask any question about how we handle your personal data, please contact our DPO.

Regulatory authority: Information Commissioner's Office (ICO) — ico.org.uk | 0303 123 1113

17. ISO 27001:2022 Compliance Controls (A.5.34) — Internal Use

This section is for internal governance purposes and documents SDS's compliance with ISO 27001:2022 A.5.34. It does not alter the privacy commitments made in Sections 1–16.

Control A.5.34 requires SDS to identify and implement measures to protect privacy and personally identifiable information in accordance with applicable law. The following internal controls are in place:

A.5.34 Requirement	SDS Control / Evidence
Identify applicable privacy and PII protection requirements	Compliance Register (updated 07/05/2026 — UK GDPR, DPA 2018, DUAA 2025, PECR)
Establish a privacy policy	This document (SDS-004 v2.0) — public-facing and internal
Document processing activities	Record of Processing Activities (ROPA) — maintained by DPO Nicole Kiezun
Assign responsibility for privacy	DPO appointed: Nicole Kiezun. Roles defined in ROPA Section 4 and this policy Section 3
Implement technical and organisational measures	Architecture Standard (v1.0), Cryptographic Controls Policy (v2.0), Access Control Policy (v2.0)
Conduct DPIAs for high-risk processing	DPIA Register maintained in ROPA Section 8. HR and payroll flagged for review
Manage subject access requests	SAR process: dpo@s-d-s.co.uk. DUAA 2025 stop-the-clock provisions applied
Manage data breaches	Incident Response Plan (v2.0). ICO notification within 72 hours where required
Assess and manage processors	Supplier/Vendor Management Policy. DPAs in place per ROPA Section 7
Provide training and awareness	Annual security and data protection training. Records held by HR
Review and audit	Annual ROPA and policy review. Internal audit programme includes A.5.34