DATA PROTECTION & GDPR POLICY

Overview

LST Projects, a trading name of LST Partnership LLP and hereafter referred to as "the Company", is committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, and the Privacy and Electronic Communications Regulations 2003 where applicable. These laws govern how the Company collects, uses, shares, stores and protects personal data relating to Employees, Clients, Contractors, Suppliers and other Stakeholders. This policy sets out the principles and procedures followed by the Company to ensure that personal data is handled lawfully, fairly, securely and transparently.

Scope

This policy applies to all personal data processed by the Company, whether held electronically or in paper form. Personal data includes any information relating to an identifiable living individual. The Company processes personal data in relation to its employees, clients, contractors, suppliers and other business contacts as part of its normal operations.

Data Protection Responsibility

The Company has appointed Anna Richardson - Office & HR Manager, as Data Protection Lead. She is responsible for overseeing compliance with data protection legislation and for providing guidance on data protection matters. The Company maintains registration with the Information Commissioner's Office where required by applicable legislation. The Data Protection Lead reports to the Managing Director, who retains overall accountability for compliance. All employees are responsible for ensuring that personal data is handled appropriately and in accordance with this policy. Any concerns or queries relating to data protection should be directed to privacy@lstprojects.co.uk

Policy Statement

The Company processes personal data in accordance with the principles set out in Article 5 of UK GDPR. Personal data is processed lawfully, fairly and transparently, and is collected only for specified, explicit and legitimate purposes. It is limited to what is necessary, kept accurate and up to date, retained only for as long as required, and protected through appropriate technical and organisational measures. These principles apply at all times and underpin the Company's approach to data protection.

Processing of Personal Data

All personal data processed by The Company is handled in accordance with a lawful basis under UK GDPR. In most cases, processing is necessary for the performance of a contract, compliance with legal obligations, or for the legitimate interests of the Company. In certain circumstances, processing may also be based on consent or other lawful grounds permitted by legislation. Where the Company processes special category data, such as health or equality information, it will do so in accordance with the additional conditions set out in legislation and will apply appropriate safeguards. The Company recognises that consent is generally not relied upon as the lawful basis for processing employee personal data, except where freely given and appropriate to do so. Employment-related processing is typically carried out to fulfil contractual, legal or legitimate business obligations.

Data Subject Rights

Individuals have rights in relation to their personal data under UK GDPR. These include the right to access personal data, to request correction or erasure, to restrict or object to processing, and where applicable, the right to data portability.

Requests may be made verbally or in writing and should be directed to the Data Protection Lead. The Company will respond within one month unless an extension is permitted. Individuals also have the right to raise concerns with the Information Commissioner's Office if they are dissatisfied with how their data has been handled.

Data Protection Complaints

Individuals may raise a complaint about the way the Company has collected, used, shared, stored or otherwise processed their personal data by contacting the Data Protection Lead at privacy@lstprojects.co.uk

The Company will acknowledge receipt of a data protection complaint within 30 days. It will take appropriate steps to investigate and respond to the complaint without undue delay, keep the complainant informed of progress where appropriate, and communicate the outcome without undue delay.

Complaints will be handled in accordance with the Company's Data Protection Complaints Procedure. Raising a complaint with the Company does not affect an individual's right to complain to the Information Commissioner's Office.

Staff Responsibilities

All staff are expected to ensure that personal data they handle is accurate, kept up to date and processed only where necessary. Personal data must be treated as confidential and must not be accessed or disclosed without appropriate authorisation. Employees are also required to report any suspected data breaches immediately to the Data Protection Lead. The Company will ensure that employees receive appropriate data protection training relevant to their role.

Data Security

The Company implements appropriate technical and organisational measures to protect personal data. Personal data must be stored securely at all times, whether in electronic or paper format. Electronic data is protected through secure systems, including password protection and encryption where appropriate, while paper records are kept in secure locations such as locked cabinets. Access to personal data is restricted to those who require it for legitimate business purposes. Any unauthorised access, disclosure or misuse of personal data may be treated as gross misconduct. The Company regularly reviews its security measures and may implement access controls, multi-factor authentication, encryption, secure backup systems and other cyber security measures appropriate to the nature of the personal data processed.

Data Retention

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected and to meet legal and regulatory obligations. Retention periods are defined within the Company's Data Retention Schedule, procedures and Privacy Notices. Personal data is securely deleted or destroyed once it is no longer required, unless the Company is required to retain it to comply with legal, regulatory or contractual obligations.

Data Breaches

A data breach occurs where personal data is lost, destroyed, corrupted, disclosed or accessed without authorisation. All suspected breaches must be reported immediately to the Data Protection Lead. The Company will investigate all breaches,

take appropriate remedial action and, where required, notify the Information Commissioner's Office within the applicable timescales. Individuals affected by a breach will be informed where there is a high risk to their rights and freedoms. All breaches will be documented and reviewed to prevent recurrence.

Accountability and Governance

The Company is responsible for demonstrating compliance with data protection legislation. It maintains appropriate records of processing activities and undertakes Data Protection Impact Assessments where required. Data Protection Impact Assessments are undertaken where processing activities are likely to result in a high risk to the rights and freedoms of individuals, including where new technologies, monitoring activities or large-scale processing of sensitive personal data are involved. Data protection is considered throughout the lifecycle of processing activities, and practices are reviewed regularly to ensure ongoing compliance.

Disaster Recovery

The Company maintains disaster recovery arrangements to ensure the integrity, availability and resilience of personal data. These arrangements include regular data backups, secure storage, system protection measures and procedures to restore access to data in the event of a disruption or system failure.

Disclosure and Sharing of Data

Personal data may be shared with third parties where necessary to fulfil contractual obligations or comply with legal requirements. This may include service providers, professional advisers, insurers and regulatory authorities. Where third parties process data on behalf of the Company, appropriate contractual arrangements are in place to ensure compliance with UK GDPR. The Company undertakes appropriate due diligence before engaging third-party processors and ensures that written data processing agreements are in place where required under Article 28 UK GDPR. Third parties are required to implement appropriate technical and organisational measures to protect personal data. Any sharing of data is carried out securely, and only the minimum amount of information necessary is disclosed.

International Transfers

Personal data will not be transferred outside of the United Kingdom unless appropriate safeguards are in place in accordance with UK GDPR, such as adequacy regulations or approved transfer mechanisms.

Freedom of Information Act (FOIA)

The Company is not directly subject to the Freedom of Information Act 2000. However, where services are provided to public sector clients, information supplied may be subject to disclosure. In such cases, the Company will cooperate with clients while taking appropriate steps to protect confidential and commercially sensitive information.

Status of this Policy

This policy does not form part of any employee's contract of employment. However, compliance with this policy is a condition of employment, and failure to adhere to its requirements may result in disciplinary action, up to and including dismissal.

Related Documents

This policy should be read alongside the following Company documents:

- Employee Privacy Notice

- Website Privacy Notice
- GDPR Data Breach Procedure
- Data Protection Complaints Procedure
- Document Retention and Archiving Process
- Information Governance Policy
- IT and Cyber Security Policy
- Access Control Policy
- Security Incident Management Policy

Policy Review

This policy will be reviewed annually, or sooner where required, to ensure it remains aligned with current legislation, industry standards and the Company's operational practices.

Shaun Tuffin
Managing Director
Last reviewed: 21st July 2026
Next review: 17th March 2027