Data Protection & Privacy Policy

This Data Protection and Privacy Policy explains how Surrey Hills Enterprises CIC ("SHE", "the Company", "we") collects, uses, stores, and protects personal data. This policy reflects the UK General Data Protection Regulation, the Data Protection Act 2018, and the Data (Use and Access) Act 2025, as amended from time to time. It applies to all employees, directors, contractors, volunteers, and anyone acting on behalf of the Company.

1. Purpose and Legal Framework

1.1 SHE is committed to protecting personal data and respecting privacy.
1.2 We comply with the UK GDPR, the Data Protection Act 2018, and related legislation.
1.3 This policy sets out how personal data must be handled and the standards expected of everyone working with or for SHE.

2. Roles and Responsibilities

2.1 The Board of Directors has overall responsibility for data protection compliance.
2.2 Day-to-day responsibility is delegated to the CEO.
2.3 All staff and directors must handle personal data lawfully, fairly, and securely.

3. Personal Data We Process

3.1 SHE processes personal data relating to employees, members, partners, suppliers, and customers.
3.2 This may include contact details, financial information, business information, images and correspondence.
3.3 We only collect data that is necessary for legitimate business purposes.
3.4 Event and Ticketing Data: SHE collects personal data from individuals purchasing or registering for tickets to events, fairs, and markets. This may include names, email addresses, postal addresses, and transaction details. This data is used to administer events, communicate essential information, meet legal and accounting obligations, and improve future events. Data is not used for unrelated purposes and is not shared except where necessary to deliver the event or comply with the law.
3.5 We may take photographs and short video recordings at events for marketing and promotional purposes, including use on our website, social media and email communications. In line with section 4 of this policy, this processing is carried out on the basis of legitimate interests

in promoting our activities and events. Individuals who do not wish to be photographed may inform a member of staff or the photographer. Individuals have the right to object to this processing and to request removal of an image where appropriate.

4. Lawful Bases for Processing

4.1 Personal data is processed only where a lawful basis applies, including:

- performance of a contract
- compliance with a legal obligation
- legitimate interests
- consent, where required

4.2 Special category data will only be processed where an additional lawful condition applies.

5. Data Security and Confidentiality

5.1 SHE implements appropriate technical and organisational measures to protect personal data.

5.2 This includes access controls, secure storage, password protection, and staff awareness.

5.3 When working from home, personal data must be protected from unauthorised access at all times.

6. Individual Rights

6.1 Individuals have rights under UK GDPR, including the right to access, correct, or delete their data.

6.2 Requests should be made in writing and will be handled within statutory timescales.

6.3 Individuals also have the right to complain to the Information Commissioner's Office.

7. Data Breaches and Incident Reporting

7.1 Any actual or suspected data breach must be reported immediately.

7.2 SHE will assess and, where required, report breaches to the ICO within statutory deadlines.

7.3 All breaches and near misses will be recorded and reviewed.

8. Payment and Financial Data

8.1 SHE does not store credit or debit card details.

8.2 Payments, including card payments and direct debits, are processed through secure third-party providers.

8.3 SHE retains only transaction records and references necessary for accounting and audit purposes.

9. Data Retention and Disposal

9.1 Personal data is retained only for as long as necessary.

9.2 Data is securely deleted or destroyed when no longer required.

9.3 Retention periods are reviewed periodically.

10. Training, Monitoring and Review

10.1 Data protection awareness forms part of staff induction where appropriate.

10.2 Compliance is monitored, and this policy is reviewed regularly by the Directors.