

## Mosspark Group

### Data Protection Policy

#### 1. Purpose

The Company is committed to protecting the personal data of employees, customers, and other stakeholders in compliance with the UK General Data Protection regulation (UK GDPR) and the Data Protection Act 2018.

#### 2. Scope

This policy applies to all personal data processed by the Company, whether stored electronically or in paper form, and to all employees, contractors and third parties acting on our behalf.

#### 3. Key Principles

The Mosspark group of companies processes personal data in accordance with the following principles:

- a) **Lawfulness, Fairness and Transparency:** Personal data will be processed lawfully, fairly and transparently.
- b) **Purpose Limitation:** Data will only be collected for specified, explicit, and legitimate purposes.
- c) **Data Minimisation:** Only the data necessary for the intended purpose will be collected and processed.
- d) **Accuracy:** Personal data will be kept accurate and up to date.
- e) **Storage Limitation:** Data will be retained only as long as necessary for its purpose or as required by law.
- f) **Integrity and Confidentiality:** Data will be processed securely to protect against unauthorised access, loss, or damage.

#### 4. Individual Rights

Individuals have the following rights regarding their personal data:

- The right to access their data.
- The right to rectify inaccurate data.
- The right to erasure ("right to be forgotten").
- The right to restrict or object to processing.
- The right to data portability.

Requests to exercise these rights should be directed to Andrew Bradbury, Data Protection Officer via HR on [humanresources@mosspark.org.uk](mailto:humanresources@mosspark.org.uk).

## **5. Data Security**

The Mossparck group of companies implements appropriate technical and organisational measures to protect personal data, including encryption, access controls, and regular security audits.

## **6. Data Breaches**

In the event of a data breach, the Mossparck group of companies will follow its Data Breach Response Plan and notify affected individuals and the Information Commissioner's Office (ICO) within 72 hours, if required.

## **7. Policy Review**

This policy will be reviewed annually or in response to changes in data protection laws.