Data Protection Statement

The Spark Group

Introduction

At The Spark Group, we value an individual's privacy and are committed to protecting personal data. This statement explains how we collect, use, store, and secure individual information in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Data Controller

The Spark Group is the Data Controller responsible for your personal data. If you have any questions, please contact us using the details provided at the end of this statement.

Types of Personal Data Collected

Given the nature of our business we may collect and process various types of personal data, such as contact details, employment information, financial details, demographic information, and any other information you provide voluntarily.

Types of Personal Data We Collect

Depending on your relationship with us (e.g. learner, employee, partner), we may collect and process:

- Contact details (name, address, phone, email);
- Employment or educational details (job role, qualifications, references);
- Financial details (payment and billing information);
- Demographic information (age, gender, preferences);
- Communications and interactions with us (emails, feedback, support requests);
- Any other information you voluntarily provide)

If we collect special category data (such as health or ethnicity), we will only do so where necessary and with appropriate safeguards.

Purposes and Legal Basis for Processing

We process your personal data for the following purposes, under these lawful bases:

Purpose	Lawful Basis
Providing and managing services	Performance of a contract

Processing payments	Performance of a contract, legal obligation
Managing customer and business relationships	Legitimate interests, contract
Communicating with you (including marketing, if applicable)	Consent, legitimate interests
Submitting funding or compliance returns	Legal obligation
Improving our services	Legitimate interests
Ensuring safety and security	Legitimate interests, legal obligation

If we rely on consent, you can withdraw it at any time by contacting us.

Data Sharing and Transfers

We may share your personal data with trusted third parties who assist us in providing our services, for example payment processors, regulatory bodies, funding agencies, professional advisors such as auditors, legal advisors. If we need to transfer your data outside the UK or European Economic Area (EEA), we will ensure appropriate safeguards are in place. We will never sell your data.

Data Retention

We keep your personal data only as long as necessary for the purposes set out in this statement or to meet legal or regulatory requirements. When no longer needed, we securely delete, anonymise, or destroy the data.

Data Security

We have implemented appropriate measures to protect your personal data against unauthorised access, disclosure, alteration, or destruction. Our security practices are regularly reviewed to ensure ongoing data protection. We take steps to ensure that anyone who processes your data does so in an authorised and secure way. We do not permit the use of removable storage devices unless specifically approved by the data controller.

Your Rights

Under data protection law, you have rights including:

- *Access* - to request a copy of your data;
- *Rectification* - to correct inaccurate data;
- *Erasure* - to request deletion of your data in some cases;
- *Restriction* - to limit processing under certain conditions;

- *Objection* - to processing based on legitimate interests or direct marketing ;
- *Data portability* - to request data transfer to another provider;
- *Withdraw consent* - where we rely on your consent

For any queries or to exercise your rights, please contact us using the details provided below.

Data Breach Response Procedure

1. Detection & Identification
We identify potential breaches through:

Google Workspace Alerts: Automatic notifications for suspicious logins, unauthorised file sharing, or bulk data downloads.

Staff Reporting: Employees are trained to report lost devices or "phishing" emails immediately to the Business Manager.

Third-Party Notification: If a sub-processor (like Google or a payment provider) notifies us of a breach on their end.

2. Containment & Recovery
Upon discovering a breach, the following immediate actions are taken:

Account Lockdown: Reset passwords and revoke active sessions for compromised Google accounts via the Admin Console.

Remote Wipe: Use Google Endpoint Management to wipe company data from lost or stolen mobile devices/laptops.

Disable Sharing: Temporarily restrict external sharing in Google Drive if a data leak is suspected.

3. Assessment (The 72-Hour Rule)
The Business Manager will assess the risk to individuals:

Low Risk: No personal data was accessed (e.g., an encrypted laptop was lost). Internal log only.

High Risk: Personal data (names, emails, financial info) was exposed. Must proceed to Step 4.

4. Notification
To the ICO: If the breach is likely to result in a risk to people's rights and freedoms, we will notify the Information Commissioner's Office (ICO) within 72 hours.

To Individuals: If the breach is "high risk" (e.g., identity theft risk), we will notify the affected individuals "without undue delay" via email.

5. Review & Record Keeping
Breach Log: Every incident (even minor ones) is recorded in our internal Data Breach Log.

Post-Mortem: We review why the breach happened and update our training or technical settings (e.g., enforcing stricter MFA) to prevent a recurrence.

Updates to this Statement

We may update this statement as needed to reflect changes in our practices or legal requirements.

Contact Information	
If you have any questions, concerns, or requests regarding this statement or our data protection practices, please reach out to us using the following details:	
Name:	**The Spark Group**
Email:	**enquiries@thespark.group**
Phone:	**07570 830068**

Approval

This policy has been approved by The Spark Group's Senior Leadership Team.

Version number:	2.1
Document written by:	Debbie Sturridge, Business Manager
Date:	23.02.26
Review due:	February 2027