Data Protection & Confidentiality Statement

The Spark Group

Introduction

At The Spark Group, we value your privacy and are committed to protecting your personal data and maintaining the confidentiality of information entrusted to us.

This statement explains how we collect, use, store, and protect your personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It also explains how we protect other confidential information relating to learners, employees, clients, commissioners, funders, partners and our business activities.

We expect everyone working on behalf of The Spark Group to handle information responsibly, share it only where authorised and report any suspected breach promptly.

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 We Collect

Depending on your relationship with us, for example as a learner, employee, partner, we may collect and process personal data such as:

- Contact details including your name, address, telephone phone and email address;
- Employment or educational details including job role, qualifications and references;
- Financial details relating to payments and billing;
- Demographic information such as age, gender and preferences, where relevant;
- Communications and interactions with us including emails, feedback and support requests;
- Other information you choose to provide or that is necessary for us to deliver our services and meet our responsibilities

If we collect special category data, such as information about health or ethnicity, we will only do so where necessary and lawful, with appropriate safeguards in place.

Purposes and Legal Basis for Processing

We process your personal data for the purposes set out overleaf, using the relevant lawful basis under data protection legislation:

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

Where we rely on your 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 support our work or where sharing is necessary to deliver our services and meet our obligations. These may include payment processors, regulators, funding agencies, Awarding Bodies, professional advisers such as auditors and legal advisers, and relevant service providers.

We share only information that is necessary and appropriate for the relevant purpose, in accordance with applicable data protection requirements and any relevant contractual arrangements.

If we need to transfer your personal data outside the UK or European Economic Area (EEA), we will ensure that appropriate safeguards are in place where required. We will never sell your personal data.

Data Retention

We keep your personal data only for as long as necessary for the purposes set out in this statement or to meet applicable legal, regulatory, funding, awarding-body or contractual requirements.

When information is no longer required, we securely delete, anonymise or destroy it, as appropriate.

Data Security

We have implemented measures to protect your personal data against unauthorised access, disclosure, alteration, loss or destruction. Our security practices are reviewed to support ongoing data protection.

We take steps to ensure that anyone who processes personal data on our behalf does so appropriately and securely. Access to information should be limited to those who need it for an authorised purpose.

Removable storage devices must not be used unless specifically approved by the Data Controller.

Your Rights

Under data protection law, you have rights in relation to your personal data. Depending on the circumstances, these include:

- **Access:** to request a copy of your personal data
- **Rectification:** to request correction of inaccurate or incomplete data
- **Erasure:** to request deletion of your data in certain circumstances
- **Restriction:** to request that the use of your data is restricted in certain circumstances
- **Objection:** to object to certain types of processing, including processing based on legitimate interests or for direct marketing
- **Data portability:** to request that certain data is provided to you or transferred to another provider
- **Withdrawal of consent:** to withdraw consent where we rely on it to process your data

If you have a question about your rights or wish to make a request, please contact us using the details provided at the end of this document.

Confidentiality

Protecting your personal data is part of our wider responsibility to maintain confidentiality. The Spark Group also handles confidential information relating to learners, employees, employers, clients, commissioners, funders, partners and other organisations. We are committed to protecting this information from unauthorised access, use or disclosure.

Confidentiality applies to information in all formats, including electronic records, paper documents, photographs, recordings and verbal conversations. Information may be confidential even if it is not marked as such.

What information is confidential?

Confidential information includes, but is not limited to:

- Learner and participant records, progress, safeguarding concerns and personal circumstances;
- Employee records and internal organisational information;
- Non-public financial information, tenders, contracts, pricing, proposals and business plans;

- Information received from clients, commissioners, funders, employers and delivery partners;
- Research and evaluation material, including interview notes, survey responses, focus-group discussions, recordings and unpublished findings;
- Passwords, access credentials and information about IT systems or security arrangements.

Information that is lawfully available to the public is not normally confidential, although other restrictions may still apply.

Handling and sharing confidential information

Everyone working on behalf of The Spark Group, including employees and sub-contractors, is expected to:

- Access confidential information only when needed for an authorised work purpose and use it only for that purpose;
- Share only the minimum information necessary, with authorised recipients and for a legitimate reason. Where possible, information should be anonymised, particularly in research, evaluation and reporting;
- Use approved work accounts, systems and storage; keep passwords private; secure devices and paper records; check email recipients and attachments; and take care that confidential conversations cannot be overheard;
- Avoid using personal email accounts, unapproved applications or unauthorised storage to hold or share confidential information;
- Not upload confidential information to public or unapproved artificial intelligence tools;
- Follow any additional confidentiality, information-sharing, publication or data-handling requirements in agreements with clients, funders and commissioners

Confidential information must not be included in public reports, presentations, case studies or promotional materials without appropriate authorisation.

Information must be retained only for as long as necessary, taking account of legal, safeguarding, funding, Awarding Body and contractual requirements. When it is no longer required, it must be securely deleted, destroyed or returned, as appropriate. Records must not be destroyed where there is a requirement to retain them, for example for safeguarding, an investigation or a contractual obligation.

Sharing confidential information

Before sharing confidential information, we must consider why it needs to be shared, whether the recipient is authorised to receive it, whether disclosure is appropriate, and how it can be shared securely.

Information must not be disclosed simply because someone has requested it or works for a partner organisation. Where a request is unclear, sensitive or unusual, anyone working on behalf of The Spark Group must check the requester's identity and authority

where appropriate and refer the matter to a member of the Senior Leadership Team (SLT).

Where information is shared with commissioners, funders, Awarding Bodies, auditors, regulators or other authorised parties to meet contractual, funding, quality assurance or legal requirements, disclosure must be limited to what is necessary and handled in accordance with applicable requirements.

For research, evaluation and consultancy projects, information must be used and shared in line with the agreed project scope and any relevant contract or confidentiality commitment. Where participants have been promised anonymity or confidentiality, reports and other outputs must be prepared carefully to reduce the risk of identification, including indirect identification through combined details.

Safeguarding and other lawful disclosures

Information may need to be shared where required by law, to meet a legitimate contractual or regulatory requirement, or where sharing is necessary and lawful to protect a child or adult at risk or prevent serious harm.

Everyone working on behalf of The Spark Group must follow our Safeguarding and Prevent Policy. Information should be shared only with appropriate people and to the extent necessary. We cannot promise absolute confidentiality where information may need to be disclosed to protect someone.

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.

Employee 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:	2.2
Document written by:	Debbie Sturridge, Business Manager
Date:	22.10.26
Review due:	February 2027