

DATA PROTECTION POLICY

Spark Projects

Table of Contents

GENERAL	3
Purpose of the policy	3
General Provisions	3
PERSONS WHOSE DATA WE MAY HOLD	4
General	4
Supporters	4
Beneficiaries	5
Spark Persons	5
DATA DEFINITIONS	6
Definitions of data protection terms	6
DATA PROTECTION PRINCIPLES	7
Introduction	7
Processing data fairly and lawfully	7
Processing data for the original purpose	8
Personal data should be adequate and accurate	8
Not retaining data longer than necessary	9
Rights of individuals under the GDPR	9
Data security	9
OTHER PROVISIONS	10
Transferring Data Outside the EEA	10
Processing Sensitive Personal Data	10
Notification	10
Monitoring and review of the policy	11
Withdrawal of Consent to Communication	11
Changes to Personal Data and Consent to Processing	11
Legislation	11

GENERAL

1. Purpose of the policy

- 1.1 This policy sets out what we do to protect individuals' personal data.
- 1.2 We are committed to processing personal data in a way that is **lawful, fair** and **transparent**. To that effect, we shall maintain this policy and comply with it when processing personal data.

2. General Provisions

- 2.1 Anyone who handles personal data in any way on behalf of Spark Projects must ensure that they comply with this policy. The *Data Definitions* section of this policy describes what comes within the definition of "personal data". Any breach of this policy may result in serious sanctions.
- 2.2 The Compliance Officer at Spark Projects oversees compliance with this policy and with the European Union's General Data Protection Regulation (GDPR). Any questions or concerns about this policy should be referred to her at compliance@sparkprojects.org.
- 2.3 In general, we process personal data of Data Subjects in the following cases: following the Data Subject's consent; to execute a contract; out of our legitimate interest; or, if compelled by Law.
- 2.4 In addition to any other actions outlined in this policy, the following steps will be taken when collecting and processing personal data:
 - (a) Spark Projects will keep a database (the "**Data Subject Directory**") with all individuals whose personal data is collected, specifying
 - the type of data,
 - the lawful basis for processing such data (e.g. consent, legitimate interests, etc)
 - when the data should be deleted
 - the date and content of consent, if applicable
 - any other opt-in or opt-out requests
 - (b) To improve data security, only the Board of Directors and the Compliance Officer will have write-access to this database.
 - (c) An up-to-date copy of our Data Protection Policy will be accessible on Spark Projects' website. Changes will be notified, by email, to all Data Subjects who provide us with an email address.
 - (d) All mass-mailed marketing communication will provide an option to opt out.
 - (e) All requests by Data Subject for erasure of personal data, change in their consent, correction of data, etc, will be promptly processed and the Data Subject's entries in the Data Subject Directory will be amended accordingly.
 - (f) Spark Projects will register with the Information Commissioner's Office as an organisation that processes personal data.
 - (g) We will keep a Data Retention Table specifying retention times per type of data.

2.5 Data Retention Table: We will retain data according *up to* the following *maximum* times:

Category of Data	Retention Period
Children Beneficiaries and their parent/carers, Supporters	While they participate in, or support, Spark and for 3 years thereafter
Applicants who did not join Spark	3 years after the application
Spark Persons, incl. volunteers	While participating in Spark and for 5 years thereafter
data with Data Subject's consent	3 years after consent is granted, except when consent is linked to an ongoing or recurring activity, in which case it is 3 years from the end of the activity.
any other data	3 years

PERSONS WHOSE DATA WE MAY HOLD

3. General

Persons whose personal data we handle (such person, a “**Data Subject**”) in running Spark Projects and its activities (“**Spark Activities**”), generally fall in the following categories:

- (a) actual or prospective volunteers and donors (“**Supporters**”);
- (b) employees, directors and volunteers (“**Spark Persons**”); and
- (c) children involved in Spark Activities (“**Beneficiaries**”), including contact details for the children's parents and carers.

4. Supporters

If you are a Supporter, we may generally collect or process your data, for the period specified in our Data Retention Table above, following your consent, to serve our legitimate interests or to execute contract.

4.1 Following your consent, for the purposes you specify

- (a) Data will be retained for the period specified in our Data Retention Table.
- (b) The Data Subject may withdraw the consent at all times (see the section *Withdrawal of Consent to Communication*). In that case, we will process the withdrawal within two weeks. We may still process some or all of your personal data if necessary to execute or honour a contract or if we are compelled to do so by law or supervisory authorities.
- (c) We will keep an up-to-date record of all consent given.

4.2 To serve our legitimate interests: We are a small charity that relies on personal contact to find supporters and deliver its services. As such,

- (a) We will contact through low-intrusion means, for example through a personal call, to discuss the work we have done, the plans we have and how you could help us.

- (b) We will also contact Supporters through mass-communication, low-intrusion means, such as infrequent emails and newsletters, to inform you of services, events and news that we believe could be of interest to you, based on your participation to related but different events and services in the past (“*soft opt-in*”).
- (c) In any case, Supporters may request not to be contacted (again, see the section *Withdrawal of Consent to Communication*).

4.3 To execute a contract: We will process your data to process or abide by a contract, e.g. to receive payment for a donation, to organize an activity you signed up for, etc.

5. Beneficiaries

5.1 We process data of Beneficiaries, that is, children participating in Spark activities, including their online activity and history, the content they create and their interaction with others.

5.2 We do so based on our legitimate interests, in order to run our activities safely and efficiently, or if required to do so by law.

5.3 We may also collect contact information for the children’s parents or carers.

5.4 We do so for a number of reasons that are critical to our activities, including

- (a) Looking out for the children’s safety, including their safety while online;
- (b) Assessing and responding to the needs and progress of individual children;
- (c) Assessing and improving Spark activities at a group level;
- (d) Monitoring whether children abide by Spark’s Acceptable Use Policy; and
- (e) Responding to incidents with children victims or perpetrators, and informing all parties necessary (their guardians, the **Host Organization** where the respective Spark activities are run, any supervisory authorities, and the police, if appropriate).

5.5 We will not share personal data of children with third parties, except if fully anonymized. We may, however, discuss personal data with a child’s parents or carers; or with appropriate Spark Persons at the respective Host Organization.

5.6 We may also share fully anonymized data, including aggregated data, with third parties. For example, we may share such data with potential partners or supporters, or to in order to present our activities to individuals or the public.

5.7 Whenever a child joins Spark, we will explain to them and their guardians how we collect and process information and for what general purpose.

5.8 Data will be retained for the period specified in our Data Retention Table.

6. Spark Persons

6.1 When someone applies to Spark Projects for a job or volunteering post, we will process that information in order to process and assess the application, as well as for recruitment statistics.

6.2 If that person does join us as an employee, volunteer, member or in some other capacity, we

will keep that person's personal information, including any additional information they provide or we obtain, but we will only use it for matters that apply directly to the engagement.

6.3 Data will be retained for the period specified in our Data Retention Table.

DATA DEFINITIONS

7. Definitions of data protection terms

7.1 The following terms will be used in this policy and are defined below:

7.2 **Data Subjects** include all living persons about whom we hold personal data, for instance an employee or a supporter. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

7.3 **Personal Data** means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in our possession). This is sometimes also referred to as *personally identifiable information*. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can also include an identifier such as an identification number, location data.

7.4 **Data Controllers** are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. Spark Projects is the data controller of all personal data that we manage in connection with our work and activities.

7.5 **Data Processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but Data Processors may include other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

7.6 **ICO** means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

7.7 **Processing** is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to:

- (a) collecting;
- (b) recording;
- (c) organising;
- (d) structuring;
- (e) storing;
- (f) adapting or altering;
- (g) retrieving;
- (h) disclosing by transmission;
- (i) disseminating or otherwise making available;
- (j) alignment or combination;
- (k) restricting;

- (l) erasing; or
- (m) destruction of personal data.

7.8 Sensitive Personal Data (which is defined as “special categories of personal data” under the GDPR) includes information about a person's racial or ethnic origin; political opinions; religious, philosophical or similar beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; biometric data; and other categories designated as special categories of personal data under the Legislation.

DATA PROTECTION PRINCIPLES

8. Introduction

8.1 Anyone processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles (summarised below), and show that we comply, in respect of any personal data that we deal with as a Data Controller.

8.2 Personal data should be:

- i. processed fairly, lawfully and transparently;
- ii. collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;
- iii. adequate, relevant and limited to what is necessary for the purpose for which it is held;
- iv. accurate and, where necessary, kept up to date;
- v. not kept longer than necessary; and
- vi. processed in a manner that ensures appropriate security of the personal data.

9. Processing data fairly and lawfully

9.1 The first data protection principle requires that personal data is obtained fairly and lawfully. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

9.2 Data is generally processed by Spark Projects, in accordance with UK and EU laws, in the following cases

- (a) Following the Data Subject's consent;
- (b) Following a contract between Spark Projects and a Data Subject (including, for example, processing a donation by the Data Subject to Spark Projects, or running an activity the Data Subject has signed up for);
- (c) To satisfy Spark Projects' legitimate or vital interests.

9.3 Fair Processing Information

- (a) When we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with the “**fair processing information**”, by telling them:

- i. the type of information we will be collecting;
- ii. who will be holding their information, i.e. Spark Projects, including contact details of the relevant officer;
- iii. why we are collecting their information and what we intend to do with it - for instance to process donations or send mailing updates about our activities;
- iv. the legal basis for collecting their information (for example, are we relying on their consent, or on our legitimate interests or on another legal basis);
- v. if we are relying on legitimate interests as a basis for processing what those legitimate interests are;
- vi. whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of their not providing that data;
- vii. the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;
- viii. details of people or entities with whom we will be sharing their personal data.

- (b) Where we obtain personal data about a person from a source other than the person his or her self, we must *additionally* provide the Data Subject with the following information:
 - i. the categories of personal data that we hold; and
 - ii. the source of the personal data and whether this is a public source.
- (c) In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must also inform individuals of their rights under GDPR, outlined in below, including the right to lodge a complaint with the ICO, and the right to withdraw consent to the processing of their personal data.
- (d) This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

10. Processing data for the original purpose

- 10.1 The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.
- 10.2 This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect an email address to update a person about our activities, it should not then be used for marketing purposes, without first getting the individual's consent.

11. Personal data should be adequate and accurate

- 11.1 The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is

inaccurate is corrected.

12. Not retaining data longer than necessary

12.1 The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased when no longer needed. If you think that we are holding out-of-date or inaccurate personal data, please speak to the Compliance Officer.

12.2 Retention times for different types of personal data are specified in the Data Retention Table..

13. Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of Spark Projects needs to be aware of these rights. They include (but are not limited to) the right:

- i. to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights);
- ii. to be told, where any information is not collected from the person directly, any available information as to the source of the information;
- iii. to be told of the existence of automated decision-making;
- iv. to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;
- v. to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;
- vi. to restrict processing where the individual has objected to the processing;
- vii. to have inaccurate data amended or destroyed;
- viii. to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else; and
- ix. to file a complaint with the UK's data protection authority, the Information Commissioner's Office (via the [ICO website](#)).

14. Data security

14.1 The sixth data protection principle requires that we keep personal data secure.

14.2 We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- 14.3** When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed. When deciding what level of security is needed, the starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.
- 14.4** The following security procedures and monitoring processes must be followed in relation to all personal data processed by Spark Projects:
- i. **Online Storage:** personal data will be saved in Spark Project's cloud storage, which is encrypted and backed up. This will be both to protect against data being stolen, as well as being lost following a physical incident.
 - ii. **No other copies:** No copies of personal data will be retained on personal computers, memory sticks, etc. All paper copies will be shredded.
 - iii. **Protection from third parties:** Spark Persons will ensure that confidential information is not visible to third parties and that they log off from their PC when it is left unattended. Personal data must always be transferred in a sufficiently secure manner. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential) and Spark Persons must keep data secure when using it outside the offices.

OTHER PROVISIONS

15. Transferring Data Outside the EEA

- 15.1** The GDPR requires that when organisations transfer personal data outside the EEA, they ensure that the data is properly protected. Please speak to the Compliance Officer.
- 15.2** The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the Compliance Officer before transferring personal data to organisations in the US.

16. Processing Sensitive Personal Data

- 16.1** On some occasions we may collect information Sensitive Personal Data (see the section on *Data Definitions*).
- 16.2** Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.
- 16.3** In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

17. Notification

- 17.1 We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the ICO where necessary when we are carrying out “high risk” processing.
- 17.2 We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

18. Monitoring and review of the policy

- 18.1 This policy is reviewed every two years by the Board of Trustees to ensure it is achieving its objectives. This policy may also be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

19. Withdrawal of Consent to Communication

- 19.1 If you wish to change how or when we communicate with you, including amending or withdrawing your consent to be contacted by us, please email us at communications@sparkprojects.org.

Where you opt out of all marketing we will not be able to use your personal data, for example to send you news of our activities and updates, except in certain limited situations, such as where required to do so by law, or to protect members of the public from serious harm. Please note that once you have opted out of marketing communications, processing of your personal data will cease for the purpose of marketing, but may not cease for other purposes for which Spark Projects retains your data, unless you also request a general termination of all processing of your personal data by Spark Projects.

20. Changes to Personal Data and Consent to Processing

- 20.1 We take the accuracy of your information seriously.
- 20.2 If you would like to inform us of a change of data, or request a copy of your personal data, please email us at personal.data@sparkprojects.org.
- 20.3 If you wish to amend or withdraw your consent for us to process your personal data for any reason, please email us at personal.data@sparkprojects.org, and we will not process your data any further, unless required to do so by law or the supervisory authorities, or in order to abide by or process a contract.

21. Legislation

- 21.1 Spark Projects is committed to complying with privacy and data protection laws including:
- (a) the General Data Protection Regulation (“**the GDPR**”) and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017;
 - (b) the Privacy and Electronic Communications Regulations (2003) and any successor or

- related legislation including, without limitation, E-Privacy Regulation 2017/0003; and
- (c) all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the ICO or any other supervisory authority (together “**the Legislation**”).