Last Full Update: August 2019 Due for Review: January 2021

NB – In line with the UK's departure from the European Union, RBF are aware there will likely be new legislation/guidance on matters of Data Protection as the GDPR is taken into UK law, therefore the usual annual review is deferred to January 2021 pending this new information.

Data Protection Statement:

"Red Balloon Foundation [RBF], in all aspects of its governance and activity, is committed to ensuring that all personal data collected about staff, service users and other individuals is collected, stored and processed in accordance with the General Data Protection Regulations [GDPR] and the provisions of the Data Protection Act 2018 [DPA]. This policy applies to all personal data, regardless of whether it is in paper or electronic format and is compliant with guidance and applicable codes of practice published by the Information Commissioners Office [ICO]."

Data Protection Definition:

The GDPR are based on six data protection principles that RBF undertakes to comply with, ensuring that all data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure.

Data Protection Policy

1. This policy understands the listed terms as follows:

1.1 'Personal Data' is any information relating to an identified, or identifiable, individual. This may include the individual's:
- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity;

1.2 'Sensitive Personal Data' is Personal Data which is more sensitive and so needs more protection, including information about an individual's:
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

1.3 'Processing' refers to anything done to Personal Data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying, either automated or manual;

1.4 'Data Subject' is the identified or identifiable individual whose Personal Data is held or processed;

1.5 'Data Controller' is a person or organisation that determines the purposes and the means of Processing of Personal Data. For the purposes of this document, the Data Controller is RBF who are registered as such with the ICO and will renew this registration annually or as otherwise legally required;

1.6 'Data Processor' is a person or other body, other than an employee of the Data Controller, who Processes Personal Data on behalf of the Data Controller;

1.7 'Personal Data Breach' refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

2. This policy applies to all team members engaged by RBF be they paid or volunteers and to external organisations or individuals working on our behalf. Specific responsibilities for different team members include:

2.1 Trustees [Board]: have overall responsibility for ensuring that RBF complies with all relevant data protection obligations;

2.2 Data Protection Officer [DPO]: is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Board and, where relevant, report to the Board their advice and recommendations on RBF data protection issues. The DPO is also the first point of contact for individuals whose data RBF processes, and for the ICO;

2.3 Directors: act as the representative of the Data Controller on a day-to-day basis;

2.4 All Team are responsible for:

2.4.1 Collecting, storing and processing any Personal Data in accordance with this policy;
2.4.2 Informing the RBF of any changes to their Personal Data, such as a change of address
2.4.3 Contacting the DPO in the following circumstances:

2.4.3.1 With any questions about the operation of this policy, data protection law, retaining personal data or keeping Personal Data secure;
2.4.3.2 If they have any concerns that this policy is not being followed;
2.4.3.3 If they are unsure whether or not they have a lawful basis to use Personal Data in a particular way;
2.4.3.4 If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
2.4.3.5 If there has been a Data Breach;
2.4.3.6 Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
2.4.3.7 If they need help with any contracts or sharing Personal Data with third parties

3. RBF undertakes to only Process Personal Data where we have one or more of the six 'lawful bases' to do so under data protection law as follows:

3.1 so that RBF can fulfil a contract with the individual, or the individual has asked RBF to take specific steps before entering into a contract;
3.2 so that RBF can comply with a legal obligation;
3.3 to ensure the vital interests of the individual e.g. to protect someone's life;
3.4 to perform a task in the public benefit in line with RBF's Constitution;
3.5 to further the legitimate interests of RBF or a third party (provided the individual's rights and freedoms are not overridden);
3.6 where the individual (or their parent/carer when appropriate in the case of a person under the age of 13) has freely given clear consent;

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018 and whenever we first collect Personal Data directly from individuals, we will provide them with the relevant information required by data protection law.

4. RBF will only collect Personal Data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data and if we want to use Personal Data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. In addition:

4.1 team will only Process Personal Data where it is necessary in order to do their jobs;
4.2 when team no longer need the Personal Data they hold, they will ensure it is deleted or anonymised as follows:

4.2.1 Basic register data (the full name of the service user and activities attended) along with End of Session Reports, Extended End of Session Reports and Safeguarding Action Reports will be stored in perpetuity for servicing evidence requests from statutory agencies;
4.2.2 Basic employment data (the full name, period of employment and disclosure and barring service information and any resultant risk assessments carried out) will be stored in perpetuity for servicing evidence requests from statutory agencies;
4.2.3 Personnel records (including line management meeting records, disciplinary/grievance information, income tax/NI/pension/payroll records) will be retained for six years after the end of the accounting period that includes the last date of the employee's work for evidence in the event of an HMRC Tax Audit and for the provision of references to future employers;
4.2.4 Emails and personal data volumes will be retained for up to six months after an employee has left RBF in order to answer queries that are contained within them;
4.2.5 Recruitment records will be retained for six months after candidates have not been successful in order to defend against tribunals or county/high court claims;
4.2.6 Donors' data including Gift Aid declarations, direct debit mandates, etc., will be retained for six years after the end of the accounting period that includes the last donation for evidence in the event of an HMRC Tax Audit, as will data relating to other individuals who make payments to RBF to access services;
4.2.7 All other data will be deleted or anonymised after a period of eighteen months after the final time that the service user engages in an RBF activity/team member leaves RBF's employment, or immediately that it is found to be inaccurate or out of date where we cannot or do not need to rectify or update it.

We will shred or incinerate paper-based records, and overwrite or delete electronic files. If a third party is used to safely dispose of records on RBF's behalf we will require the third party to provide sufficient guarantees that it complies with data protection law.

4.3 where team are going to be processing data in a new way, a Data Protection Impact Assessment must be completed (see Appendix B) and reviewed by the DPO and a member of the RBF Leadership Team before data collection and Processing can begin.

5. RBF will only share Personal Data where:

5.1 there is an issue with a service user or parent/carer that puts the safety of our staff or other service users at risk;
5.2 we need to liaise with other agencies due to a Safeguarding or other similar issue, and, where appropriate, we will seek consent from concerned parties as necessary before doing this;
5.3 our suppliers or contractors need data to enable us to provide services to our service users – for example, IT companies. When doing this, we will:

5.3.1 only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
5.3.2 establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any Personal Data we share;
5.3.3 only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us;

5.4 we are legally required to do so, including for:

5.4.1 the prevention or detection of crime and/or fraud;
5.4.2 the apprehension or prosecution of offenders;
5.4.3 the assessment or collection of tax owed to HMRC;
5.4.4 in connection with legal proceedings;
5.4.5 where the disclosure is required to satisfy our safeguarding obligations;
5.4.6 research and statistical purposes, as long as Personal Data is sufficiently anonymised or consent has been provided;

5.5 we are assisting emergency services and local authorities to help them to respond to an emergency situation that affects any of our service users or staff;
5.6 we are delivering services on behalf another party, such as a church, and so we are acting as that other party's agent. In these cases, both the third party and RBF will act as Data Controllers, but RBF undertakes to ensure that similar provisions to those outlined in 5.3.1 and 5.3.2 are in place before any data is shared and explicit consent from service users is received.

6. Where RBF transfers Personal Data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

7. RBF recognises the right of individuals to make a 'subject access request' [SAR] to gain access to personal information that we hold about them.

7.1 This includes:

7.1.1 confirmation that their Personal Data is being processed;
7.1.2 access to a copy of the data;
7.1.3 the purposes of the data processing;
7.1.4 the categories of Personal Data concerned;
7.1.5 who the data has been, or will be, shared with;

7.1.6 how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
7.1.7 the source of the data, if not the individual;
7.1.8 whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

7.2 SARs must be submitted in writing, either by letter or email to the DPO, and, if other staff members receive a SAR, they must immediately forward it to the DPO. SARs should include:

7.2.1 name of individual;
7.2.2 correspondence address;
7.2.3 contact number and email address;
7.2.4 details of the information requested.

7.3 RBF affirms that Personal Data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR, but the DPO will assess this on a case-by-case basis.

7.4 When responding to requests, RBF will:

7.4.1 ask the individual to provide two forms of identification;
7.4.2 contact the individual via phone to confirm the request was made;
7.4.3 seek clarification where necessary in order to provide the highest quality and most relevant information to the individual making the request;
7.4.4 will respond without delay and within one month of receipt of the request;
7.4.5 will provide the information free of charge.

7.5 RBF will not disclose information if it:

7.5.1 might cause serious harm to the physical or mental health of the service user or another individual;
7.5.2 would reveal that a child or vulnerable adult is at risk of abuse, where the disclosure of that information would not be in the child/adult's best interests;
7.5.3 is contained in adoption or parental order records;
7.5.4 is given to a court in proceedings concerning the children;
7.5.5 if the request is unfounded or excessive particularly if it is repetitive, or asks for further copies of information already provided.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8. RBF also recognises the rights of individuals to:

8.1 withdraw their consent to Processing at any time;
8.2 ask us to rectify, erase or restrict processing of their Personal Data, or object to the Processing of it (in certain circumstances);
8.3 prevent use of their Personal Data for direct marketing;
8.4 challenge Processing which has been justified on the basis of public interest;
8.5 request a copy of agreements under which their Personal Data is transferred outside of the European Economic Area;
8.6 object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);

8.7 prevent Processing that is likely to cause damage or distress;
8.8 be notified of a Data Breach in certain circumstances;
8.9 make a complaint to the ICO;
8.10 ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances);

Individuals should submit any request to exercise these rights to the DPO. If team receive such a request, they must immediately forward it to the DPO.

9. RBF uses CCTV in various locations around various premises we make use of to ensure our team, service users and the premises themselves remain safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the DPO.

10. As part of our activities, RBF may take photographs and record images of individuals taking part in our activities and:

10.1 we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and child. Where images are taken/recorded at large events where this explanation is not possible, we will prominently display notices detailing how photographs/videos may be used;
10.2 we recognise consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further;
10.3 when using photographs and videos we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

11. RBF undertakes to put measures in place to show that we have integrated data protection into all of our data processing activities, including:

11.1 appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
11.2 only processing Personal Data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
11.3 completing privacy impact assessments where RBF's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies per the template below;
11.4 integrating data protection into internal documents including this policy, any related policies and privacy notices;
11.5 regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters;
11.6 regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
11.7 maintaining records of our processing activities, including:

11.7.1 for the benefit of Data Subjects, making available the name and contact details of RBF and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);
11.7.2 for all Personal Data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. RBF will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage by ensuring:

    12.1 paper-based records and portable electronic devices, such as laptops and hard drives that contain Personal Data are kept under lock and key when not in use;
    12.2 papers containing confidential Personal Data must not be left unattended anywhere else where there is general access;
    12.3 passwords that are at least 8 characters long containing letters, numbers and punctuation are used to access RBF computers, laptops and other electronic devices and team are reminded to change their passwords at regular intervals;
    12.4 encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
    12.5 all team who store personal information on their personal devices are expected to follow the same security procedures as for RBF-owned equipment;
    12.6 where we need to share Personal Data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

13. All team members are provided with this policy and are given access to appropriate training as part of their induction process, and data protection will also form part of continuing professional development, where changes to legislation, guidance or the RBF's processes make it necessary.

Appendix A: Personal Data Breach Procedure

A1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO, who will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

A1.1 lost;
A1.2 stolen;
A1.3 destroyed;
A1.4 altered;
A1.5 disclosed or made available where it should not have been;
A1.6 made available to unauthorised people;

A2. The DPO will alert the Directors and Chair of Trustees and work with them to make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or Data Processors where necessary, carrying out the following actions:

A2.1 assessing the potential consequences, based on how serious they are, and how likely they are to happen;
A2.2 working out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

A2.2.1 loss of control over their data;
A2.2.2 discrimination;
A2.2.3 identify theft or fraud;
A2.2.4 financial loss;
A2.2.5 unauthorised reversal of pseudonymisation (for example, key-coding);
A2.2.6 damage to reputation;
A2.2.7 loss of confidentiality;
A2.2.8 any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

A2.3 documenting the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. This should include the facts associated with the Breach including its cause and effects and the agreed actions taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

A3. Where the ICO must be notified, the DPO will do this via the 'report a breach' page on the ICO website within 72 hours. As required, the DPO will set out:

A3.1 A description of the nature of the personal data breach including, where possible the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned;
A3.2 the name and contact details of the DPO;
A3.3 a description of the likely consequences of the personal Data Breach;
A3.4 a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned;

If any of the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

A4. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

A4.1 the name and contact details of the DPO;
A4.2 a description of the likely consequences of the personal Data Breach;
A4.3 a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned;

A5. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

Appendix B: Data Protection Impact Assessment Template

B1. A form based on the template below must be completed by any team wishing to Process Personal Data in a new way not currently carried out by RBF.

Name of Project

DPIA Rationale

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Processing Outline

Nature of Processing

- *How will you collect, use, store and delete data?*
- *What is the source of the data?*
- *Will you be sharing data with anyone?*
- *What types of processing identified as likely high risk are involved?*

Scope of Processing

- *What is the nature of the data, and does it include special category or criminal offence data?*

- *How much data will you be collecting and using and how often?*
- *How long will data be kept for it?*
- *How many individuals are affected?*
- *What geographical area does it cover?*

Context of Processing

- *What is the nature of your relationship with the individuals?*
- *How much control will they have?*
- *Would they expect you to use their data in this way; do they include children or other vulnerable groups?*
- *Are there prior concerns over this type of processing or security flaws? Is it novel in any way?*
- *What is the current state of technology in this area?*
- *Are there any current issues of public concern that you should factor in?*

Purpose of Processing

- *What do you want to achieve?*
- *What is the intended effect on individuals?*
- *What are the benefits of the processing for you, and more broadly?*

Consultation & Links with Stakeholders

- *Describe when and how you will seek individuals' views –or justify why it's not appropriate to do so.*
- *Who else do you need to involve within your organisation?*
- *Do you need to ask your processors to assist?*
- *Do you plan to consult information security experts, or any other experts?*

Compliance and Proportionality

- *What is your lawful basis for processing?*
- *Does the processing actually achieve your purpose?*
- *Is there another way to achieve the same outcome?*
- *How will you prevent function creep?*
- *How will you ensure data quality and data minimisation?*
- *What information will you give individuals and how will you help to support their rights?*
- *What measures do you take to ensure processors comply?*
- *How do you safeguard any international transfers?*

Data Risk Assessment

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

Explain any terms/acronyms used here:

Risk	***Persons Affected***	***Rating****	***Measures in Place***	***Further Mitigating Action***

**Note on Ratings*

1. All individual items on a risk assessment are to be allocated a risk rating by:
    a. Assigning a number that represents the likelihood of the risk happening: 1 (seldom), 2 (frequently), 3 (certain or near certain).
    b. Assigning a number that represents the severity of injury that is likely to occur if the risk comes about: 1 (minor cuts and bruises), 2 (serious injury or incapacitation for 3 days or more), 3 (fatality or multiple persons seriously injured).
    c. Multiplying those two numbers together to produce a final risk rating.
2. Additional safety measures will therefore be prioritised according to risk rating as follows:
    a. 1-2: Low Priority

   b. 3-4: Medium Priority
   c. 6-9: High priority.
3. Therefore:
   a. A low priority risk may require no or minimal action.
   b. A medium priority risk may require some additional measures to be implemented.
   c. A high priority risk may require activities to be suspended/restricted until action has been taken.