GDPR and Data Protection Policy

5 Point Plan (see term definitions on page 3):

1. BRF holds data that is necessary to carry out its work and in line with legal obligations (Includes organisational data, personal data and occasional sensitive data)
2. All staff personal data is held on the HR Drive, which is only accessible by the CEO, administrator and line managers.
3. All personal data is obtained with the individual's consent, and is handled in line with the GDPR principles (page 4). Individuals are informed what the purpose of holding this data is, and if this data will be shared with anyone/third parties etc.
4. Individuals can make formal requests for the data BRF holds on them. BRF will only share data requested by a 3rd Party if in line with legal requirements set out in sections 7 and 8.
5. BRF minimises the amount of personal data it retains by checking folders/platforms/documents every January, and deleting data that is no longer required

Policy Contents:

1. Policy statement
2. About this policy
3. Definition of data protection terms
4. Data protection principles
5. Notifying data subjects
6. Processing in line with data subject's rights
7. Disclosure and sharing of personal information
8. Dealing with subject access requests

1. POLICY STATEMENT:

Bristol Refugee Festival is registered under the Data Protection Act and with the ICO. Bristol Refugee Festival is required to process relevant personal data regarding team members, suppliers,

stall holders, traders, sponsors, artists and performers, volunteers and people interested in volunteering as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Bristol Refugee Festival recognises The Data Protection Act 1998 and The General Data Protection Regulation (GDPR) adopted in 2016 (tailored by the Data Protection Act 2018)

Detailed Statement:

1. BRF holds three types of information which are covered by this policy:
    a. organisational information – publicly available information about organisations and some individuals within organisations
    b. personal information – information about individuals (including stakeholders, partners, attendees, volunteers and employees) such as names, email address and job titles
    c. sensitive personal information – in general this kind of information is only held about employees and volunteers. There are, however, instances where sensitive information is held about other people. For example, information about members' dietary requirements that the festival might allow a person's religion to be deduced.

    *Note that Information about organisations is not covered by the Data Protection Act.
2. Bristol Refugee Festival will not hold information about individuals without their knowledge and consent.
3. Bristol Refugee Festival will only hold information for specific purposes. It will inform individuals what those purposes are and will inform them if those purposes change.
4. Information will not be retained once it is no longer required for its stated purpose.
5. Bristol Refugee Festival will seek to maintain accurate information by creating ways in which people can update the information held. Email notifications should be sent to info@bristolrefugeefestival.org for action.
6. Information will be retained within Bristol Refugee Festival and will not be given to third parties. Individuals will only receive newsletters and notifications from Bristol Refugee Festival that will communicate on the activities and purposes of Bristol Refugee Festival and on related local topics.
7. Individuals are entitled to have access to information held about them by Bristol Refugee Festival.
8. Information about individuals will not be disclosed to other organisations or to individuals who are not Bristol Refugee Festival team members except in circumstances where this is a legal requirement, where there is explicit or implied consent, or where the information is publicly available elsewhere.

9. Bristol Refugee Festival uses 3rd party hosted applications, such as Google applications, Whatsapp and Mailchimp, to conduct its business. Data used by these applications may be stored outside of the EEA.
10. Bristol Refugee Festival has procedures for ensuring the security of all personal data. Paper records containing confidential personal data are disposed of in a secure way. Electronically held personal data will be protected from unauthorised access.
11. There may be situations, where Bristol Refugee Festival works in partnership with other organisations, such as stakeholders, funders and sponsors, which may require some data sharing. Personal data will not be shared, but overall statistics, for example on attendance numbers may be shared.
12. Bristol Refugee Festival employees and volunteers will be given training on Bristol Refugee Festival data protection policy and procedures.
13. Bristol Refugee Festival employees and volunteers must not download any personal or sensitive data on their personal devices. If in the course of their work they are required to do so they must delete this information immediately.
14. Bristol Refugee Festival employees and volunteers should not undertake their work on public unsecured wifi. Ideally work must only be accessed on a private / password protected wifi network. Exercise caution when remote working in a public space.
15. Bristol Refugee Festival employees and volunteers must not input personal or sensitive information e.g. names, emails, phone numbers, into AI.
16. Bristol Refugee Festival will carry out regular reviews of its data protection policy and procedures.

2. ABOUT THIS POLICY

2.1 This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.2 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.3 The CEO is responsible for ensuring compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the CEO and/or the Board.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on Bristol Refugee Festival's behalf.

3.7 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. GDPR PRINCIPLES

Bristol Refugee Festival has used the following principles to inform this policy

4.1 Lawfulness, Fairness and Transparency
You must have the right to process the data, it must not compromise the data subject, and everyone needs to be clear about what is being done. This is 95% of GDPR. Much hinges on individual definitions of “fair”, “lawful” and “transparent” but most people will know a failure of one of these when they see it.

4.2 Purpose Limitation
Be clear and upfront about this, and obtain a legal gateway for each purpose

4.3 Data Minimisation
Only process the data you need to. This means having the data you actually need to do the processing accurately (including contextual data) - but only that data, and being clear on why the data is needed for the stated purpose

4.4 Accuracy
Don’t process data which is inaccurate. Although this seems obvious, data quality is a big problem in a lot of organisations due to input errors, processing glitches, or simply data getting old. ICO say you “should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact”.

4.5 Storage Limitation
Only keep the data for as long as you need it. Once you’ve used the data for your stated purposes, let it go. GDPR requires that this is made explicit in a policy document and you should be able to obtain consent or some other legal basis for holding the data for this length of time. We have this in our GDPR Record of Processing Activity document https://docs.google.com/spreadsheets/d/1OfXjOB4MI9zlJPMtQG6BCUeb_FJQw7I8iMgKjIVrVh4/edit?usp=sharing

4.6 Security
Keep the data safe. Data must be held securely and the integrity and confidentiality of that data needs to be protected.
We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes.

4.7 Accountability

You are responsible for maintaining the privacy of personal data. Take responsibility for what you do with personal data to comply with the other principles. Keep records of what you do and why

5. NOTIFYING DATA SUBJECTS

5.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

5.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

5.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

5.4 We hold a GDPR Record of Processing Activity, which outlines the data sets we hold and what they are used for. This can be found and updated here: https://docs.google.com/spreadsheets/d/1OfXjOB4MI9zlJPMtQG6BCUeb_FJQw7I8iMgKjlVrVh4/edit?usp=sharing

6. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

6.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also Clause 15).
(b) Prevent the processing of their data for direct-marketing purposes.
(c) Ask to have inaccurate data amended (see also Clause 9).
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

7.1 We may share personal data we hold with any member of our group, if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, partners, volunteers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8. DEALING WITH SUBJECT ACCESS REQUESTS

8.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees and volunteers who receive a written request should forward it to the CEO immediately and make no agreement regarding the request themselves. Organisations have **one calendar month** to respond to a subject access request (SAR) under UK GDPR. The one-month period starts on the exact day the organisation receives your valid request.

a) Under the Data (Use and Access) Act 2025 (DUAA), organisations can formally pause ("stop the clock") while they wait for necessary clarification from you regarding what data you are seeking

8.2 We cannot give personal information via telephone enquiries and will ask the caller puts their request in writing. Employees and volunteers should make no agreement regarding the request themselves.

8.3 If the organisation fails to respond within the time frame, data subjects can file a formal complaint with the organisation or escalate the issue directly to the ICO Online Complaint Form.