Be More Foundation: Data Protection Policy

Overview

Be More Foundation (BMF) values the data that is provided to us, and we endeavour to keep any information provided to us safely and securely. Access is only provided to those that have a legitimate interest in that data.

"Personal Data" means recorded information we hold from which an individual can be identified.
"Processing" means doing something with that data, such as accessing, using, or disclosing.

Data protection principles

We will comply with the data protection principles as set out in Article 5 of the General Data Protection Regulations, which requires that data shall be;

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a matter that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) Processed in a manner that ensures appropriate security of the personal data, including protections against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

"Personal data" means recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, and expressions of opinion about you or indications as to our intentions about you. "Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

Fair and lawful processing

There are 6 lawful bases for processing personal data under the General Data Protection Regulations (GDPR);

- Consent – the data subject has freely given consent for their information to be processed for a specific purpose
- Contract – processing is necessary due to the fulfilment of a contract
- Legal Obligation – processing is necessary to comply with the law
- Vital Interest – processing is necessary to save or protect an individual's life
- Public Tasks – processing is necessary to perform a public interest in official functions
- Legitimate Interests – processing is necessary to the legitimate interests of an organization or a third-party affiliate.

We will usually only process your personal data where you have given your consent or where the processing is necessary to comply with our legal obligations. In other cases, processing may be necessary for the protection of your vital interests, for our legitimate interests or the legitimate interests of others.

We will only process "sensitive personal data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the DPA.

How we are likely to use your personal data

We will process data about staff for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits connected to your employment.

We may process sensitive personal data relating to staff including, as appropriate:

1. information about an employee's physical or mental health or condition in to monitor sick leave and take decisions as to the employee's fitness for work;
2. the employee's racial or ethnic origin or religious or similar information to monitor compliance with equal opportunities legislation;
3. to comply with legal requirements and obligations to third parties.

Processing for limited purposes

We will only process your personal data for the specific purpose or purposes notified to you or for any other purposes specifically permitted by the DPA.

Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

Accurate data

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

Data retention

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

You have the right to:

1. Request access to any personal data we hold about you;
2. Prevent the processing of your data for direct-marketing purposes;
3. Ask to have inaccurate data held about you amended;
4. Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else;
5. Object to any decision that significantly affects you being taken solely by a computer or other automated process.

HR and Employment Records:

- Applications etc from unsuccessful candidates: will be kept on file for a maximum of 6 months post closing date of advertisement.
- General Employee Records; These should be kept for 6 years following the end of the employment relationship. This covers items such as CVs and application forms, details of qualifications, contract of employment, changes to job title, notes of disciplinary and grievance hearings, information about promotions and reporting lines etc
- Working time & Annual Leave records: 2 years from the period to which they relate

- Family Leave records: no more than 3 years after the end of the tax year in which the relevant pay ends
- Payroll and Wage records: no more than 6 years from the end of the financial year in which the payments were made
- DBS Checks & Disclosures; Retained for 6 years following the termination of the employment relationship, as relevant to the ongoing employment relationship
- Statutory Sick Pay Records – 3 years after the end of the tax year in which the statutory sick pay period ends
- Return to work forms and GP / Consultant Records: 6 years from the date on which the employees employment with FFP ends.

Funders Information

- Grant Agreements; kept for 6 years after the funding relationship ends

Members Information

- Due to the nature of services we provide, and young people that we support, we will retain on file the information of those who join BMF indefinitely.
- Should a Young Person request that we remove them from our data stores, we shall.

Financial Records

- ANNE – ask about archiving policy / process

Data security

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

Providing information to third parties

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

Subject access requests

The General Data Protection Regulation gives individuals the right to access personal data held by BMF, including the right to obtain confirmation that we process their personal data, receive information about what we do with such data, and obtain a copy of personal data BMF holds.

To access this information, the individual needs to send a request to info@fightforpeace.net containing the following information;

- Proof of Identity (such as passport, photographic ID, birth certificate)
- Details of information requested, such as employment records, data held by certain departments, correspondence etc.

We will then be able to provide information including;

- The purposes of processing
- The types of personal data processed
- How long we store the data, or criteria for determining retention periods
- Your right to request correction or deletion of data; restrict or object to certain types of processing; make a complaint.

BMF may require further information from the Requestor to be able to process their request. We will aim to respond within one month of the request being made.

Breaches of data protection principles

BMF undertake data audits on a regular basis to ensure that the data we hold is secure. We use password protected online filing systems, and hard copies of documents are accessible by authorised key holders only. Access to data is only granted to those within the Charity who have a legitimate interest in accessing the data to undertake their role within BMF.

If you become aware of a breach, or a potential breach, you must immediately bring this to the attention of your line manager and the Head of Programmes.

Where there is a potential breach, BMF will undertake an immediate investigation. Such investigation will be undertaken by the Chief Operating Officer, Head of Programmes and Governance Officer.

The Security Breach team shall;

- Investigate the potential breach, including the nature and cause of the breach, and the extent of the damage or harm that could result.
- Take immediate action to stop or mitigate the breach
- Consider the need to report to the Information Commissioners Office
- Consider the need to contact the individuals affected by the breach
- Review the cause of the breach, whether there is any claim or liability due to the breach
- Review the data protection security policies and procedures.

Privacy Notice

How we use your personal data:
BMF are committed to protecting your personal data. We will use your information to provide our services to you, or to comply with our legal obligations. We process the information you give to us with your consent, or where necessary for out legitimate interests in providing our services.

Disclosure of your data
We may have to share your personal data with those who provide our IT, database, and Monitoring, Evaluation and Learning systems. We ensure all of these third parties respect the security of your data, and treat it in accordance with the law.

Data Security
Keeping your information safe is very important to us. We have put in place systems to stop your information from being lost, used or accessed in an authorised way, altered or disclosed. We also ensure your information can only be accessed by those who have a business need to know, and who have a duty of confidentiality. We may anonymise your information, so you can no longer be identified, for research and statistical purposes. We may use this information indefinitely.

Data Retention
We will keep your personal information for as long as necessary to fulfil the purposes for which it was collected. We may retain your data for reporting requirements for up to 6 years after you cease to be a member.

Your Rights
You have the right to request any information we hold about you - a Subject Access Request - please speak to a member of staff, or email us at info@fightforpeace.net

Complaints
If you are not happy with any aspect of how we collect and use your data, you can complain to the Information Commissioner's Office; www.ico.org.uk

We would ask that you contact us first, so we can try and resolve any issue for you first.