BRITISH PSYCHOTHERAPY FOUNDATION

Registered charity number 115080

data protection policy

policy statement

The British Psychotherapy Foundation (*bpf*) will ensure that it complies with both the law and good practice in all its dealings with personal data which it holds on individuals. In particular, the *bpf* will respect the rights of individuals and be open and honest with those whose data is held, provide appropriate training and support for staff and members who handle personal data and follow the data protection principles of good information handling which are set out in the General Data Protection Regulation (GDPR) (EU) regulation on data protection and privacy.

Article 5 of the GDPR requires that personal 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 manner 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 organisational 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 protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Under the Act, *bpf* is the Data Controller in respect of personal data which it holds. The *bpf* is registered with the Information Commissioner's Office and the registration number is ZA000986.

requirements

As required by Article 5(2), the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

At the ***bpf***, the Chief Executive is responsible for ensuring that the ***bpf*** complies with its legal obligations in respect of the Act. Operational responsibility is delegated to the Data Protection Officer.

Any contractor working for the ***bpf*** must be placed under an obligation to comply with data protection requirements as a term of their contract for services with the ***bpf***.

personal data of members and trainees

The ***bpf's*** Membership Application Form will include information on data protection so that, in signing-up, the prospective member or trainee consents to the organisation holding and processing Personal Data including Sensitive Data. Application forms for training will include a similar provision.

personal data of employees

The ***bpf's*** Contract of Employment for staff provides that staff give their consent to the organisation holding and processing Personal Data including Sensitive Data.

personal data of prospective patients and patients

Consent to the ***bpf*** holding and processing Personal Data including Sensitive Data will be obtained from prospective patients and patients by means of a declaration on the information forms which they are required to complete.

definition of data and sensitive data

Data is defined as information that is:

- Processed automatically or manually by computer databases;
- Recorded with the intention of processing by computer;
- Recorded as part of a paper filing system;
- Any information that forms part of an accessible record not covered by the above definitions.

Sensitive data is defined as information on the person's:

- Racial or ethnic origin;
- Political opinions;
- Religious belief;
- Culture;
- Age;
- Membership of a trade union;
- Physical or mental health;
- Sexual life;
- Offences committed or alleged to have been committed.

Explicit permission must be obtained from the person concerned for sensitive information to be processed. Consent will normally be obtained via the Membership Application Form (for Members and Trainees) or Contract of Employment or otherwise obtained in writing, for example via information forms for patients and prospective patients, agreements with self-employed contractors and equalities monitoring forms for job applicants.

subject access requests

People whose personal data is held by the ***bpf*** are entitled to see their personal data, by sending a written request to the Data Protection Officer. This is known under the Act as a 'Subject Access Request.' Where the individual making a Subject Access Request is not known to the ***bpf's*** Data Protection Officer or another member of staff or a Board or Committee member, their identity will be verified before information is handed over. The ***bpf*** may charge the fee which is applicable under the Act at the time for providing access to data. The Act requires the ***bpf*** to respond to a Subject Access Request within 40 calendar days of receiving it.

Under the Act, an individual who makes a written request is entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the information comprising the data; and
- Given details of the source of the data (where this is available).

There is some data which is exempt from the Act and where this applies, information about the reasons for the exemption will be provided.

disclosure of information to third parties

Personal information will normally be disclosed for the reason why the data is held, such as provision of services. Otherwise, information may be disclosed at the request of the Data Subject, for example, a request from an employee for a financial reference.

Where an official request for disclosure of personal information is received this will only be done in compliance with the law and with the authorisation of the Data Protection Officer. In such circumstances, it may be appropriate not to inform the Data Subject, for example where fraud is suspected. All such disclosures will be documented.

data security

The General Manager will be the Data Protection Officer.

The Chief Executive is responsible for:

- Briefing and advising the Board on data protection matters;
- Reviewing this Data Protection Policy;
- Advising other staff on data protection issues;
- Issuing operational procedures for data handling within the British Psychotherapy Foundation;
- Ensuring that data protection training (including induction) takes place;
- Notification to the Information Commissioner and maintaining the registration;
- Handling Subject Access Requests;
- Approving disclosure of personal data as described in item 8 above.

The Data Protection Officer will identify specific risks in relation to data security and issue operational procedures designed to mitigate and manage any risks including, but not limited to the following areas:

- Access to the *bpf's* IT system;
- Network and web site security;
- Locking/logging off from personal computers when away from the desk;
- Security of personal passwords;
- Who in the British Psychotherapy Foundation has access to which databases;
- Password protection of files;
- Encryption of laptops;
- Use of memory sticks;
- Hard copies and information held electronically;
- Backing up of information;
- Dealing with telephone or email requests for information about individuals.

data accuracy

The Data Protection Officer will issue operational procedures to ensure that, as far as possible, personal information held by the British Psychotherapy Foundation is accurate. These procedures will include but not be limited to:

- Where data is recorded and stored;
- Data on any individual to be held in as few places as possible and all relevant systems to be updated when information about an individual changes;
- Regular checking that information is still accurate, updating, retention periods, discarding and archiving.

induction and training

The *bpf* will develop suitable induction materials so that staff coming into the organisation are aware of their Data Protection responsibilities, provide training updates for staff and ensure that all staff receive appropriate induction and on-going training.

The *bpf* will develop suitable procedures and guidelines for members involved in providing training and delivering other activities so that they are aware of their Data Protection responsibilities and provide training.