British Porphyria Association

136 Devonshire Rd
Durham City
County Durham
DH1 2BL
Charity No: 1089609
www.porphyria.org.uk

Subject Access Request (SAR) Policy

The British Porphyria Association (BPA) aims to ensure that individuals are aware of their right to ask for a copy of the records that the BPA hold about them.

The BPA Privacy Policy enables individuals to understand how to ask what data is held about them and how to correct or remove that data.

This SAR Policy aims to ensure that subject access requests are dealt with in an appropriate and timely manner by the BPA.

Confidentiality

All SAR information will be handled sensitively, telling only those who need to know and following any relevant data protection requirements.

Responsibility

Overall responsibility for this policy and its implementation lies with the board of trustees and the executive committee.

Review

This policy is reviewed regularly and updated as required.

Adopted on: Mar 2019

Last reviewed: May 2020

Signed: ..... J Chamberlayne ..... Name .....John Chamberlayne.....

Position: .....BPA Chair.....

Subject Access Request (SAR) Procedure

A subject access request applies to all personal data held by the BPA. The request can be made by an individual regarding their own data or on behalf of someone else.

1. Ensure the subject access request is valid.

A valid subject access request is one which:

- provides all the information required to locate the information the person wants
- provides sufficient information to verify the data subject's identity.

If all relevant information is not provided, you must write to the data subject for more information.

The BPA has one month to provide the information requested once all the necessary information has been received. This deadline can be extended with agreement of the individual.

2. Verify the data subject's identity

Before disclosing any personal information, you must verify the identity of the data subject.

Whilst it is important that you do not send copies of personal information to people who are not the data subject, you must not appear obstructive.

Data Protection legislation requires you to take 'reasonable measures' to verify the identity of a data subject. You can often verify their identity from their circumstances, such as their address or signature.

3. Further verification

If you require further verification of the data subject's identity you have two options.

- Verify identity by phone – see sample below
- Verify identity in writing – write to the individual and ask them to send you a photocopy of their passport or drivers licence (this option will take longer and it is also possible that the individual does not have a passport or drivers licence).

4. Calculate the target date

You have one month from receipt of a valid request to provide the information. If the request was made on the 31st October, then a response would be expected by 30th November.

5. Find relevant information

Instigate a search of the BPA database, Gift Aid records, JustGiving records and committee correspondence files/emails. Sample email to committee at the back of this guide.

6. Screen the information

- Not all personal information may be liable for disclosure. Providers of the information will have done an initial screening but you will need to check it. Blank out exempt and/or irrelevant information.
- Check the data subject. Check that the record is actually about the person concerned and not about someone else with the same name. For example, an email might carry the subject line 'Meeting about Tom Smith' but if the email only contains details about whether people can attend the meeting, the email is not about Tom Smith.

- Screen out duplicate records or data about other individuals.

7. Keep a record

Log any queries in the database.

Create a file for each subject access request and keep: copies of the correspondence between yourself and the data subject, and between yourself and any other parties; a record of any telephone conversation used to verify the identity of the data subject; a record of decisions; copies of the information sent to the data subject. The file should be kept for one year and then securely destroyed.