



Records Management and Document Retention Policy

This policy is a commitment from the British Porphyria Association (BPA) to take proper care of the records it holds and to comply with the European Union General Data Protection Regulation (GDPR). This policy applies to all records created and maintained by trustees, committee members or volunteers in the course of carrying out its functions.

Our policy is to ensure that:

- only relevant (lawful) information is collected
- individuals know what personal data is collected and why
- records are only used for the purposes declared
- individuals know their rights: e.g. how to ask what data is held about them and how to correct that data
- individuals maintain the right to be forgotten
- records are accurate and up to date
- records are not kept any longer than necessary
- records are kept secure and confidential
- any data breach is handled appropriately
- the BPA committee is appropriately trained

What type of information is collected by the BPA?

It is necessary to keep certain records to comply with the BPA's legal and regulatory obligations and to enable the effective management of the charity. These records are relevant and legitimate in implementing the main aims of the organisation: to support and educate patients, relatives and clinicians about porphyria, and to promote research.

We obtain information about individuals when they contact us via the email or telephone helpline, when they make a donation, when they fundraise or volunteer for us, or if they become a member.

Personal data collected might include an individual's name, address, email address, telephone number, type of porphyria and donation details. We also collect financial information relating to donations/subscriptions. Finally, records of consent, subject access requests and correspondence via email or letter will also be collected.

How is this information used?

Information is used to:

- communicate with members
- help respond to queries
- process donations

- support fundraisers or volunteers
- administer the charity effectively and efficiently
- seek views or comments on the services provided

Information usage is explained clearly in the **BPA Privacy Policy** which will be updated annually to take into account any changes.

Who has access to this information?

Only members of the BPA committee that need to process, monitor or audit personal data will have access to this information. In certain instances, information may be accessed by reputable third parties to process BPA services, such as sending out newsletters.

We will never sell or rent out personal information to third parties.

Obtaining consent

Individuals have a choice about whether or not they wish to receive information from the BPA as well as how they would like to receive that information. Consent is requested from all individuals connected to the BPA.

- Individuals are asked to positively opt in using a paper form or via an online form.
- Individuals are informed of their right to revoke their consent at any time.
- The BPA keeps a record of when the consent was obtained.
- The BPA regularly reviews consents to check that the data, processing and purposes have not changed and renews consents when required.

Subject access request (SAR) and right to be forgotten

Individuals have the right to ask for a copy of the records that the BPA hold about them. They also have the right to ask for all records the BPA hold about them to be removed. The **BPA Privacy Policy** ensures that individuals know how to ask what data is held about them and how to correct or remove that data.

SAR procedure

The **BPA Subject Access Request (SAR) Policy** and procedure document contains a step-by-step guide and sample letters. Also, see <https://ico.org.uk> for the Information Commissioner's Office code of practice.

- **Initial questions:** is the request valid? Can the identity of the subject be verified?
- SARs must be responded to within 40 days of receipt.
- A SAR will instigate a search of the BPA database, Gift Aid records, JustGiving records and committee correspondence files/emails.
- A SAR response will include the following: details of whether any personal data is held; a description of the personal data and the reason it is being held; a copy of the personal data; and the source of the data (where this is available).
- Volunteers will be trained on how to recognise and respond to SARs in an annual training/review session.
- The BPA keeps a record of when the SAR was requested.

Right to erasure procedure

The **BPA Right to Erasure Policy** and procedure document contains a step-by-step guide and sample letters.

- A request to have personal data erased will be responded to immediately.
- If the data is no longer necessary for the purpose for which it was collected or processed, or if the data subject withdraws consent to the processing and there is no other legal basis for the processing, the data must be erased.
- Volunteers will be trained on how to respond to erasure requests in an annual training/review session.
- The BPA keeps a record of when the erasure was requested.

Keeping records safe and secure

The BPA works hard to ensure that security precautions are in place to protect the loss, misuse or alteration of information. Processes for doing so involve the following:

Paper-based documentation processes

- Records are filed immediately after printing
- Locked cabinets are used for paper-based files
- Crosscut shredding to be used for confidential waste

Electronic documentation processes

- Anonymous file names used when saving personal records
- Strict user permissions are maintained for the membership database
- BPA committee to use specific email folders for member related correspondence
- All committee members must adhere to minimum requirements for password complexity: All passwords should contain upper and lower case letters and a number(s).
- Transfer to Windows 365 for secure file storage and sharing, plus cloud storage.
- Virus software to be installed and kept up to date on all BPA committee systems, including portable devices.

Email processes

- Emails containing personal details will be kept by the BPA no longer than is necessary.
- Emails containing personal data will be deleted by the BPA five years after they have been received or sent. However, certain emails may be kept for longer periods (including indefinitely, if this is in the best interest of the charity).
- BCC (blind carbon copy): if emails are sent by the BPA to more than one individual on the database, then the BPA will use BCC. This ensures that the names of the recipients are kept private and no one within that email will receive the email addresses of anyone else.
- Marketing: marketing emails will only be sent to parties who have opted-in to receive such emails.

Keeping records up to date

We are legally required to hold some types of information to fulfil our statutory obligations (for example, the collection of Gift Aid). We only hold personal information on our systems for as long as is necessary.

We review the length of time we keep personal information on a regular basis. Every 12 months the BPA reviews what personal data it holds, the sources of personal data held and who it is shared with by way of the **BPA Information Audit**.

Document retention

The below document retention schedule and **BPA Information Audit** sets out how long the BPA needs to keep certain types of records and provides guidance as to how information should be disposed of.

| Type of record | Length of time retained | Format of record | Disposal action |
|--|---|---|--|
| Membership records | Until requested to remove or returned mail received | Access database | Delete |
| Gift Aid declarations | Six complete calendar years after last gift claimed on the declaration – then destroy | Paper-based Electronic/database | Shred Delete |
| Financial records: forms, statements, invoices, etc. | The default standard retention period for HMRC records is 6 years plus current, otherwise known as 6 years + 1. | Paper-based accounts Excel spreadsheets | Shred Delete |
| Donation and fundraiser records, including JustGiving and Virgin Money | The default standard retention period for HMRC records is 6 years plus current, otherwise known as 6 years + 1. | Paper-based records Excel spreadsheets Database | Shred Delete Remove donor/fundraiser |
| Correspondence, incl emails, from individual members Meeting/open day records | Date of correspondence + 5 years (maximum) – then destroy | | |
| Minutes Annual reports and accounts | Kept indefinitely | | |

Data breaches

The BPA Committee need to know about incidents involving any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. E.g.

- unauthorised access to or disclosure of personal data or confidential BPA information
- lost or stolen laptops, smart phones, memory sticks or other IT equipment containing personal data

Please see the **BPA Data Breach Policy** for more information and procedures to follow in the event of a data breach.

Training and awareness

An annual training session for BPA committee will review the principles relating to charity administration, data protection and records management. The BPA keeps a record of training sessions. Each session will include:

- Principles on the processing of personal data
- How data is collected, processed and audited
- How to ensure data is relevant, accurate and up to date.
- Dealing with a subject access request, including verifying the identity of the individual making the request
- Data security principles
- Reporting a potential breach

Nominated person

The BPA has nominated an individual to monitor compliance with GDPR. This will be reviewed annually.

Confidentiality

All 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* NameJohn Chamberlayne.....

Position:BPA Chair.....

