



GDPR Policy including Records Retention and Privacy Notice

My Breast Cancer Support

Policy Owner - Alison McGrath
Policy Approved by: My Breast Cancer Support Trustees
Date Policy Approved: 9 December 2024
Next Review Date: December 2027

Document Version Control

Date	Version	Amendments Made	Trustee making changes
9/12/2024	New	Creation of Document	Alison Newton

Certification of Current Version

Certified By	Signature	Role	Date
Trustee Sara Williamson		Chair	9 December 2024
Trustee Alison McGrath		Trustee	9 December 2024

Introduction

This policy outlines My Breast Cancer Support commitment to data protection and compliance with the UK Data Protection Act. The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of My Breast Cancer Support, including trustees and volunteers.

Purpose of the Policy

This policy will set out the actions and processes that My Breast Cancer Support Trustees will follow to ensure the GDPR regulations are fully met. It will specify what members, supports and volunteers can expect from the Board in relation to Data Protection. Additionally our processes will be detailed to ensure transparency with regard to our data processing and use of the data provided to the group.

Data Protection Lead

My Breast Cancer Support will appoint a Data Protection Lead (Alison McGrath) who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all trustees and volunteers are provided with any induction and made aware of their data protection responsibilities.

Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is UK law which regulates the processing of personal data. The UK Information

Commissioner's Office (ICO) provides guidelines on data protection that MY Breast Cancer Support Group will follow.

- **UK GDPR:** The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
- **Data Processor:** An individual or organisation that processes personal data on behalf of a data controller.
- **Data Controller:** An individual or organisation that determines how and why personal data is processed.
- **Data Subject:** An individual whose personal data is being processed.
- **Processing:** Any operation performed on personal data, including collection, storage, use, and disclosure.
- **Personal Data:** Any information that can identify a living individual, such as name, address, or email address.
- **Sensitive Personal Data:** Personal data that requires extra protection, such as health information or ethnic origin.
- **Direct Marketing:** Any communication aimed at promoting a product or service directly to an individual.
- **PECR:** The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.
- **Valid Consent:** Consent given freely, specifically, and informed, and can be withdrawn at any time.
- **Legitimate Business Purpose:** A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

Data Protection Principles

Data is:

- **Processed lawfully, fairly and in a transparent manner.**
 - There are several grounds on which data may be collected, including consent.
 - We are clear that our collection of data is legitimate and we have obtained consent to hold an individual's data, where appropriate.
 - We are open and honest about how and why we collect data and individuals have a right to access their data.
- **Collected for specified, explicit and legitimate purposes and not used for any other purpose.**
 - We are clear on what data we will collect and the purpose for which it will be used.
 - And only collect data that we need.
 - When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.
- **Adequate, relevant and limited to what is necessary.**
 - We collect all the data we need to get the job done.
 - And none that we don't need.
- **Accurate and, where necessary, kept up to date.**
 - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.

- We correct any mistakes promptly.
- **Kept for no longer than is necessary. We understand what data we need to retain, for how long and why.**
 - We only hold data only for as long as we need to.
 - That includes both hard copy and electronic data.
 - Some data must be kept for specific periods of time (eg accounting, Health and Safety).
 - We have a Records Retention process that ensures data no longer needed is destroyed.
- **Processed to ensure** appropriate security, not only to protect against unlawful use, but also loss or damage.
 - **Data is held securely**, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected.
 - **Data is kept safe.** Our IT systems have adequate anti-virus and firewall protection that's up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
 - **Data is recoverable.** We have adequate data back-up and disaster recovery processes.

Data Breach - General Information

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where there will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence. We will notify the ICO within 72 hours, of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- Result in discrimination.
- Damage to reputation.
- Financial loss.
- Loss of confidentiality or any other significant economic or social disadvantage.

Special Category Data

Special category (sensitive) data is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Privacy And Electronic Communications

Known as PECR, there are special regulations covering electronic marketing messages (by phone, fax, email or text), cookies and electronic communication services to the public.

Fundraising

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors.

Artificial Intelligence

At this point My Breast Cancer Support have made a conscious decision not to use AI in the creation of any policies procedures or funding bids. We will take further advice and anything that is developed will comply with the [Charity AI Ethics and Governance Framework](#) and ICO AI guidance.

Individual Rights

We recognise that individuals' rights include the right to be informed, of access, to rectification, erasure, restrict processing, data portability and to object.

My Breast Cancer Support Privacy Notice

My Breast Cancer Support is a breast cancer peer support network and a registered charity and is committed to protecting and respecting the privacy of its members, supporters and volunteers. We provide practical and emotional support to those with a breast cancer diagnosis primarily within the Mid Yorkshire NHS area although we have members from other NHS trusts. The lawful basis on which My Breast Cancer Support holds personal data is that of consent, ie:- explicit consent is given by its members, volunteers and supporters in order to store their personal data. My Breast Cancer Support use personal data to provide the services and information that its members sign up to when joining and also to communicate with supporters and volunteers about events and activities. Personal data is not shared with any other third party unless; it is anonymised as general data for statistical purposes as detailed in our GDPR Policy or the information gives us concern for the safety and welfare of our members, the individual the information is about or their families, in which case the information will be passed on to the relevant authority in line with our Safeguarding Policy.

What Personal Data we Hold

Members will be required to give information via our Membership Form in order to join My Breast Cancer Support. There are two types of information that we may hold. Compulsory information that we require is name, date of birth, next of kin, address, contact details and communication preferences. Optional information such as breast cancer related medical details can be provided in order to assist us in tailoring support towards the individual, ie passing on relevant research and information that may be relevant.

Personal data of members, supporters and volunteers may also be obtained by corresponding with us by telephone, e-mail or via social media.

Why we Need your Personal Data

The reason we need personal data is to be able to process and administer the membership of My Breast Cancer Support, provide the support services that members sign up to when joining and communicating with supporters and volunteers regarding events and activities.

Reasons we need to process your data include:

- To administer the membership of My Breast Cancer Support including
 - The processing of membership forms.
 - Sharing data with the Trustees in order to organise events and activities and provide specific, requested support.
 - My Breast Cancer Support Newsletter distribution.
 - Communication regarding My Breast Cancer Support events with members, supporters and volunteers.

Social Media

My Breast Cancer Support has a closed group on Facebook (My Breast Cancer Support) which members have the option to join. Members should be aware that by joining this group all other members of that closed group will have access to the information that they post within it. Before joining the group members should ensure that their own Facebook privacy settings are in place to meet their individual needs. Should an individual member choose to become Facebook friends with another member of the closed group, therefore allowing that friend access to the information contained within their Facebook account, they should be aware that they do so at their own risk and My Breast Cancer Support take no responsibility for an individual's privacy settings outside of the closed group.

Accountability and Governance

Where we Store Personal Data

Personal data will be stored in locked, fireproof cabinets (for paper records) at the My Breast Cancer Support registered address and that of the Secretary (the Data Processor). Electronic copies of membership forms and spreadsheets will be securely kept using cloud hosting, protected by password security which is accessed only by specific trustees of My Breast Cancer Support (Chair, Treasurer, Secretary and Policy and Compliance Officer). The Data Processor will ensure that spreadsheets and databases are updated as soon as consent is received. Where telephone numbers of members, supporters and volunteers has been given to My Breast Cancer Support, Trustees as part of their role these will be deleted from personal devices if a member ceases their membership of the group either in person or following their death once advised by family members.

Who we Share your Personal Data With

My Breast Cancer Support does not share any personal data it holds with any other third party. Occasionally My Breast Cancer Support may share anonymised group statistics (eg how many members have a specific breast cancer type) in the interests of breast cancer research and living with and beyond breast cancer service development or My Breast Cancer Support funding applications.

My Breast Cancer Support data processing requires personal data to be transferred outside of the UK for the purpose of cloud hosting. Where My Breast Cancer Support does transfer personal data overseas it is with the appropriate safeguards in place to ensure the security of that personal data.

Records Retention

My Breast Cancer Support will hold personal data on its members for the duration of their membership. Any personal data we hold on members will be securely destroyed upon request to cease membership at any time, in accordance with the GDPR 'right to be forgotten'. In the case of supporters and volunteers, communication in writing is required in order for My Breast Cancer Support to delete the personal data held. Personal data is not processed for any further purposes other than those detailed in this policy. When we are informed of a death of a member their records will also be removed from the database. Removal of member records will also take place from the closed Facebook group, although on death these will remain active for one month following the death of a member should the family wish to advise of funeral arrangements via a trustee of the group.

Your Rights Regarding your Personal Data

As a data subject, members, supporters and volunteers have the right at any time to submit a subject access request in order to access a copy of the personal data that My Breast Cancer Support holds about that individual. This request should be made in writing via post or email and My Breast Cancer Support will comply with any such requests within one month of receipt.

Complaints can be made to the Information Commissioner's Office, about the processing of your personal data. As a data subject you are not obliged to share your personal data with My Breast Cancer Support, however if you choose not to share your personal data with us we may not be able to register or administer your membership. In the case of supporters and volunteers we may be unable to communicate regarding events and activities.

Data Breaches

A data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Should any member, volunteer or supporter detect a data breach, they are obliged to inform the Data Officer (My Breast Cancer Support Secretary) in the first instance. Additionally, they have the right to complain to the ICO. My Breast Cancer Support will regularly update and change all passwords relating to personal data protection in order to avoid potential data breaches.

Data Breach Procedure

The Data Officer will undertake an investigation which will include making arrangements to gather all necessary information from the reporting individual or organisation. An emergency meeting of the Trustees will be called and the complaint will be investigated within one month. The Data Officer will inform the ICO and any individual that may be affected of any breaches they are aware of. The Trustees may choose to review the policy as an outcome of the investigation.

Use of Photographs and Video footage

Where photographs or video footage of My Breast Cancer Support members is to be used to promote the group or provide an update on an event that has been held consent will be sought from all involved before any images are published. Where images contain children or vulnerable adults explicit consent for a particular photo or video will be gained before making this public. All members of My Breast Cancer Support will be asked to sign a consent form with regard to images when they become a member of the group. However where third parties are involved in the production of any images additional consent will be obtained at this time.

Help And Support

The regulator, the Information Commissioner's Office (ICO) has produced guidance for charities [here](#), or to contact the ICO by phone, e mail or live chat, click [here](#). You can find a self-assessment tool and other resources for micro, small and medium sized organisations [here](#).