HEART SUPPORT GROUPS DATA PROTECTION GUIDE

The British Heart Foundation (BHF) is the nation's heart charity, dedicated to saving lives every day by investing in pioneering research, supporting and caring for heart patients and their families, campaigning for change and providing vital information to help people care for their own heart health.

As part of your work as a Heart Support Group, you will handle Personal Data and you are expected to take care of it and comply with the GDPR. The GDPR governs all actions taken in relation to Personal Data; it recognises two types of data:

Personal Data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data – any information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. This category of personal data is given an extra level of protection.

WHAT THE GDPR SAYS

Anyone processing Personal Data must comply with the six GDPR principles of good practice. Personal Data must be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
3. adequate, relevant and limited to the purposes
4. accurate and up-to-date
5. not kept in a form that permits identification of the data subjects for longer than necessary for the purpose
6. processed in a manner that ensures appropriate security of the personal data

WHAT YOU NEED TO DO

- Understand why Data Protection is important.
- Only collect information you need and use it for the purpose you've collected it. Do not use it for any other purpose.
- Provide information on a need to know basis- limit disclosure of Personal Data.

SECURE IT

- Secure files and papers containing Personal Data at all times; never leave information about group members lying round.
- Secure Personal Data held on computers by password protecting the files and the computer. When emailing people, for group purposes use the Bcc field to protect the addresses of other group members.
- When sending attachments containing Personal Data (e.g. a spreadsheet), ensure the spreadsheet is password protected and send the password in a separate email or by telephone.
- Ensure that specific information which could identify an individual is not made public.

SHRED IT

- Always shred or destroy Personal Data securely after use; don't just put it in a bin.

✓ **GETTING IT RIGHT - Proper handling of Personal Data shows respect for people's information and fosters confidence in your Heart Support Group.**

✗ **GETTING IT WRONG - Poor handling of Personal Data could lead to bad publicity and loss of reputation.**

FURTHER INFORMATION

The Information Commissioner's Office (ICO) is responsible for enforcing the GDPR. Their website **www.ico.org.uk** has a wealth of the resources on data protection; in particular this guidance created for not-for-profit groups **https://ico.org.uk/media/for-organisations/documents/1567/exemption-from-registration-for-not-for-profit-organisations.pdf**

FIGHT FOR EVERY HEARTBEAT

bhf.org.uk

Registered charity numbers 225971 & SC039426