ME ASSOCIATION DATA PROTECTION AND PRIVACY POLICY

Introduction

Both the ME Association (MEA) and ME Connect are legally required to comply with the Data Protection Act 2018, all extant legislation in being and the General Data Protection Regulations.

Part 1 of this Policy outlines the main points relating to the work of ME Connect's volunteers but it is important to read this document in its entirety. Volunteers are required to sign a Data Protection Form.

Part 2 of this document outlines the Policy that applies to all who provide work to the MEA. If callers ask about Data Protection you can refer them to this entry on www.meassociation.org.uk - click on 'About Us", then click on "We're here for you" and then scroll down to 'Policies and Documents' and finally click on 'Data Protection and Privacy Policy'.

In addition, the MEA requires all who provide work to it to abide by the Data Security-working from home guidance which is available on the MEA's internal data system held on One Drive

There is an important point we need to remember. Any request for personal information from us has to be made for a 'proper purpose'. An example here would be asking for a caller's address if they have requested an information pack. Other information we ask for such as ethnic origin or whether the caller is a member or not is not personal information, the statistics here are anonymised.

PART 1 – Guidelines for volunteers

This list is not inclusive, please read the data protection principles reprinted below.

- Only write full names and address on your log sheet if the caller wants an Information Pack. Never write an email address or telephone number on your log sheet, they are not required.
- When you email either ME Connect's office or the MEA office your email may contain sensitive information or information which could identify a person. You will thus need to delete the email you sent as soon as you have received a response.
- You must make sure that names and addresses (or other personal details of callers) are not kept on your hard drive.
- To ensure that sensitive information or information that could identify a person is

'safe', you must have comprehensive and up to date anti virus protection on your computer.

- Do not under any circumstances dial 1471 after a call
- Caller display is not allowed but we appreciate that you may need this on your phone therefore we ask that you do not look at it when you are working with ME Connect
- Log sheets are kept securely. Initially in ME Connect's office and within 3 months of the call at the MEA office. Log sheets are shredded after 12 months bearing in mind that 'information shall not be kept longer than is necessary'.
- Volunteers should not keep copies of their log sheets or any notes containing details that could identify a caller.
- The log sheets only contain information which the caller has consented to give us and provided both MEC and the MEA only use that data for the purpose for which it was given and keeps it safe and confidential then we are not in breach of the Act.

CONCLUSION – to Part 1

To summarise and conclude this section, please always ask yourselves the following questions:

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?
- Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
- Is access to personal information limited to those with a strict need to know?
- Am I sure the personal information is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?

Answering 'Yes' to all these questions does not completely satisfy the Act and we need to be constantly aware that data needs to be protected and emails virus free. Please now carefully read the website statement below.

PART 2 – The ME Association Website Statement

ME ASSOCIATION DATA PROTECTION AND PRIVACY POLICY

What information we collect

Personal data you provide We collect data you provide to us. This includes information you give when joining or registering, placing an order or communicating with us. For example: • personal details (name, email, address, telephone etc.) when you join as a member • financial information such as bank details (we do not keep payment information such as credit/debit card) and are legally required to keep declarations as to Gift Aid • information created by your involvement with the ME Association Your activities and involvement with the ME Association will result in personal data being created. This could include details of how you've helped us by volunteering or being involved with our campaigns and activities.

Sensitive personal data We do not collect or store sensitive personal data. However, there are some situations where this is necessary (e.g. if you volunteer with us). If this does occur, we'll take extra care to ensure your privacy rights are protected.

How we use information We only ever use your personal data to: • enter into, or perform, a contract with you; • comply with a legal duty; • contact you with information of legitimate interest • protect your vital interests; • for our own (or a third party's) lawful interests, provided your rights don't override these. As an example, we use personal data to communicate with people, to promote the ME Association, and to help with fundraising. This includes keeping you up to date with our news, updates, campaigns and fundraising information. We also use personal data for administrative purposes (i.e. to carry on our charity and fundraising work). This includes: • receiving donations (e.g. gift-aid declarations); • maintaining databases of our volunteers, members and supporters; • performing our obligations under membership contracts; • fulfilling orders for goods or services (whether placed online, over the phone or in person); • helping us respect your choices and preferences

Disclosing and sharing data We will never sell your personal data. We may share personal data with subcontractors or suppliers who provide us with services. For example, if you order something from the ME Association Shop, your name and address will be shared with the delivery company or where a mailing company needs your name and address to deliver your quarterly magazine. We are also legally required to inform HM Revenue and Customs as to Gift Aid.

Fundraising As a charity, we rely on donations and support from others to continue our work. From time to time, we will contact members and supporters with fundraising material and communications. This might be about an appeal, a competition we're

running, or to suggest ways you can raise funds (e.g. a sponsored event or activity, or even buying a product if the ME Association will receive some of the proceeds).

How we protect data We employ a variety of physical and technical measures to keep your data safe and to prevent unauthorised access to, or use or disclosure of your personal information. Electronic data and databases are stored on secure computer systems and we control who has access to information (using both physical and electronic means). How long we store information We will only use and store information for so long as it is required for the purposes it was collected for. How long information will be stored for depends on the information in question and what it is being used for. We continually review what information we hold and delete what is no longer required. 7.

Keeping you in control We want to ensure you remain in control of your personal data. Part of this is making sure you understand your legal rights, which are as follows: • the right to confirmation as to whether or not we have your personal data and, if we do, to obtain a copy of the personal information we hold (this is known as subject access request); • the right to have your data erased (though this will not apply where it is necessary for us to continue to use the data for a lawful reason); • the right to have inaccurate data rectified.

Complaints You can complain to the ME Association directly by contacting us using the details set out above. If wish to make a complaint which does not directly relate to your data protection and privacy rights, you can do so in accordance with our charity's complaints policy. If you are not happy with our response, or you believe that your data protection or privacy rights have been infringed, you can complain to the UK Information Commissioner's Office which regulates and enforces data protection law in the UK. Details of how to do this can be found at www.ico.org.uk

Cookies and links to other sites Cookies .Our website uses local storage (such as cookies) to provide you with the best possible experience and to allow you to make use of certain functionality (such as being able to shop online). Links to other sites Our website contains hyperlinks to many other websites. We are not responsible for the content or functionality of any of those external websites (but please let us know if a link is not working). If an external website requests personal information from you (e.g. in connection with an order for goods or services), the information you provide will not be covered by the ME Association's Privacy Policy. We suggest you read the privacy policy of any website before providing any personal information. When purchasing goods or services from any of the businesses that our site links to, you will be entering into a contract with them (agreeing to their terms and conditions) and not with the ME Association.

THE ME ASSOCIATION AND THE DATA PROTECTION ACT 2018

The ME Association is extremely conscious of the importance of keeping all data it holds confidential. All persons who handle any data on its behalf have clear guidelines as to how that data must be handled. In particular the eight principles set out below and contained in The Data Protection Act 2018 are our touchstone.

Data Protection Principles

The Eight Data Protection Principles are based on three key concepts:
Purpose – personal data must only be held for a clear purpose or purposes;
Fairness – personal data must only be processed for legitimate purposes;
Transparency – data subjects must be given certain basic information about the personal data held about them.

First Principle – fair and lawful processing
"Personal data shall be processed fairly and lawfully and shall not be processed unless certain conditions are met."
This Principle aims to ensure that individuals are made aware of how their personal data will be used and covers both the original obtaining of data, for both computer and manual files, and its subsequent processing.

Second Principle – purposes for holding data
"Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes."
This Principle covers the identification of the purposes for which data is processed and the restriction of processing to those purposes.

Third Principle – status of data
"Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed."
This Principle requires that all data held must be justified in relation to the stated purpose for which it is held. In collecting data therefore it is important to ask whether the data is really needed for the purposes concerned. If the answer is no, the data must not be collected. It is equally important to review the amount of data being collected from time to time to ensure that it is still relevant.

Fourth Principle – accuracy of data
"Personal data shall be accurate and, where necessary, kept up-to-date."
This Principle requires that the data held is always accurate and, except in the case of historic data kept for archive purposes, up-to-date.
In holding data therefore procedures must be put in place (i) to ensure that data is accurate and (ii) to enable data to be updated.

Fifth Principle – retention and disposal of data
"Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose or those purposes."
This Principle covers the retention of data for the purpose concerned and its subsequent disposal. No data must be kept for longer than is necessary to carry out the purpose concerned. The length of time will vary greatly with the type of data being held; in some cases it might be appropriate to retain it for only a very short time, in other cases it might be necessary to retain it indefinitely; some retention periods are even governed by statute.
Once a retention policy is in place, appropriate procedures to dispose of the data must also be put in place. Security is very important in the disposal of personal data.
If data is to be retained for archive purposes, the Third Principle must be taken into account.

Sixth Principle – rights of data subjects
Personal data shall be processed in accordance with the rights of data subjects under the Act.
This Principle covers a number of rights which data subjects have with respect to their own data. These are (i) rights of subject access, (ii) rights to prevent processing, including direct marketing, (iii) rights of compensation for substantial damage or distress, (iv) rights to have data amended or deleted, and (v) rights relating to automated decision-taking.
Subject access: Data subjects have the right to have access to their personal data. This is probably the most important of the data subject rights. It is also the right of which most data subjects are aware.
Prevention of processing including direct marketing: The Act includes an important right to prevent processing, in particular direct marketing. This relates to any information sent out to a data subject that is not directly concerned with our business. For example, flyers sent about unrelated products for sale by a third party. Anyone likely to engage in direct marketing must have procedures in place to enable a data subject to object to being the target of direct marketing and to have their name removed from any such lists.

Seventh Principle – disclosure of data
"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."
This Principle covers both the disclosure of data and the unauthorised or unlawful processing of data. It is probably the single most important Principle and the easiest to

get wrong. Data security is another way of looking at disclosure and is equally important as far as the Seventh Principle is concerned. Various measures must be taken to ensure that data is kept secure:
Technical measures: network security; the proper use of passwords;
Organisational measures: the physical security of computers and files in cabinets; locked rooms; ensuring that computer screens cannot be overlooked.
Accidental loss, destruction or damage to data has the same effect as an unauthorised disclosure. Good back-up procedures must be in place and used effectively. These should include procedures to recover lost data.
It is particularly important to be aware of data security when processing data offsite, especially when using a laptop in a public place such as a train.

Eighth Principle – transfer of data
"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."
The ME Association

PART 3 - FREEDOM OF INFORMATION ACT
Very occasionally people ask whether it is possible to have access to the ME Association's Register of Members. On other occasions people ask about a certain member. If you are asked for such information then please use the information below.

It is important to note that the MEA is not subject to the Freedom of Information Act and so can refuse requests made under the Act. The Act covers organisations in the public sector such as Government Departments. The charity is, however, obliged to allow access to its 'members list' but here the request for information has to be made for a 'proper purpose'. The basis for any disclosure of details is about the rights attached to the shares and not the members themselves. The MEA complies with the strict provisions of the Companies Act 2006.

VERSION 02/12/2022