The ME Association Limited
Data Protection Policy

PURPOSE

This document sets out the key requirements with which the ME Association (the charity) must comply in relation to data protection, as set out in applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018),The Privacy and Electronic Communications Regulations 2003 (PECR) and the Data(Use and Access) Act 2025 (DUA) This Policy is separate to our privacy notices, which are found on our websites, and our employee privacy notice (available internally to employees).

This document sets out:

- How we will ensure compliance with the UK GDPR, DPA 2018, the PECR and the DUA
- Our roles and responsibilities that are relevant to internal compliance, and that all business areas understand their responsibilities in relation to data protection matters
- How our compliance with this Policy will be monitored.

SCOPE AND APPLICATION

This Policy provides a framework to demonstrate how the charity will comply with its obligations and responsibilities to information covered by UK Data Protection Legislation. This Policy is supported by various internal policies and procedures. The UK GDPR definition of "Personal Data" includes any information relating to an identified or identifiable natural living person. Pseudonymised Personal Data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 2018, providing the anonymisation has not been done in a reversible way.

This Policy is mandatory. It is managed by our Data Protection Officer (DPO) and applies to all the processing of Personal Data carried out by the charity, including processing carried out by joint controllers, contractors, processors, and all individuals working for, or on behalf of it. Failure to comply with this Policy or any of the other processes or policies referred to within it could lead to appropriate and proportionate punitive action.

OUR RESPONSIBILITIES

The section below sets out the principles and key requirements of the UK GDPR, which guide all business areas, to ensure that the processing of Personal Data is carried out fairly and lawfully, without adversely affecting the rights of individuals; the permitted use of the charity's Personal Data is also detailed in this Policy. The charity will:

- Appoint a Data Protection Officer to undertake the tasks set out in Article 39 and to support compliance
- Adhere to the seven principles set out in Article 5 of the UK GDPR
- Always have a lawful basis under Article 6 for processing Personal Data, and also under Article 9 when processing special category data
- Have an Appropriate Policy Document to meet the specific conditions of the DPA 2018, when processing special category or criminal offence data
- Restrict the use of the charity's Personal Data, only to those who require access to fulfil their roles
- Restrict access to the charity's Personal Data to the level of least privilege to enable staff to fulfil their roles
- Uphold the rights of data subjects
- Implement measures to prevent the misuse of the charity's Personal Data
- Implement measures to ensure data protection by design and by default
- Ensure, where possible, we use pseudonymisation and anonymisation to protect the charity's Personal Data
- Comply with rules on automated decision making and profiling
- Ensure all direct marketing is compliant with the PECR and UK data protection laws
- Keep records of our processing activities in line with Article 30

- Provide data protection awareness information to all staff and carry out audits for compliance with this Policy
- Maintain privacy notices to detail how and why we process Personal Data
- Only use data processors who offer appropriate safeguards and comply with UK data protection laws
- Only share the charity's Personal Data where there is a lawful basis to do so
- Not transfer Personal Data outside Europe without appropriate safeguards and controls
- Appropriately record all breaches and near misses, and report those meeting the threshold for reporting
- Ensure appropriate accountability, responsibility, and governance for processing the charity's Personal Data
- Review this Policy annually.

INFORMATION GOVERNED BY UK DATA PROTECTION LEGISLATION

The charity's Personal Data is: information relating to any charity employee or customer data, or data of any other individuals we interact with, which is processed (any action involving that data including viewing, using, sharing saving etc) on any HR, customer, business developed or procured systems, and any file shares, shared email inboxes, employee made spreadsheets, databases, third party systems, cloud-based systems, data shared with third parties and data stored in reporting or dashboarding applications etc.

The charity processes Personal Data for specific purposes, for employment purposes and to enable it to provide services to its members and the general public, which are detailed in our privacy notices. The UK GDPR requires that we process Personal Data in a way that ensures appropriate security of that data, including protection against unauthorised access, unlawful processing, accidental loss, destruction, or damage. The charity has implemented technical safeguards, policies and procedures to protect against these risks.

APPOINTMENT OF A DATA PROTECTION OFFICER

We appoint a Data Protection Officer and provide them with adequate resources to undertake their tasks. These tasks will typically include:

- The provision of advice and guidance for complying with UK data protection laws to the controller, processors and employees who undertake processing activities,
- Monitoring compliance
- Providing training and providing advice and guidance on DPIAs
- Cooperating and acting as the single point of contact with the Information Commissioner on issues relating to processing, prior consultation and where appropriate, regarding any other matter.

If you have any questions about this Policy, please raise them with The charity's DPO.

THE PRINCIPLES

The sections below set out the principles and a more detailed look at the key requirements of the UK GDPR. The charity adheres to the seven principles of the UK GDPR as set out in Article 5. This means that:

1. Personal Data is processed lawfully, fairly and in a transparent manner. *(Lawfulness, fairness and transparency principle)*
2. Personal Data is used for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. *(Purpose limitation principle)*
3. Personal Data is adequate, relevant, and limited to only what is necessary for the purpose for which it is being processed. *(Data minimisation principle)*
4. Personal Data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified without undue delay. *(Accuracy principle)*
5. Personal Data is kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data are processed. *(Storage limitation principle)*

6. Personal Data is kept in a manner that ensures appropriate security of that data, including protection against unauthorised access or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. *(Integrity and confidentiality principle)*
7. For The charity to be able to evidence its responsibilities and demonstrate compliance with all the principles set out in 1 to 6 above *(The Accountability principle)* we have appropriate and effective measures to ensure the business complies with data protection law; failure to follow these could result in breaches of legislation, action from our regulator (IC), reputational damage, loss of confidence by data subjects and financial implications.

LAWFUL BASIS

To process personal data in compliance with all the principles of the UK GDPR, an appropriate lawful basis under Article 6 must be identified; an additional lawful basis is also required under Article 9 if we are processing special category data.

APPROPRIATE POLICY DOCUMENT

In some circumstances where we are processing special category data, we are required under Schedule 1, Part 2, of the DPA 2018, to have an internal Appropriate Policy Document in place to cover those processing activities. We have an Appropriate Policy Document to cover the processing of special categories of Personal Data in certain circumstances.

USE OF THE CHARITY PERSONAL DATA

Only individuals who have access to the charity's Personal Data, as part of their job role, are authorised to use this data. Their authorisation is for official business only. Individuals follow all established charity policies and procedures when accessing personal data and the charity systems.

ACCESS PERMISSIONS

Individuals who require access to the charity databases containing Personal Data are authorised with the least level of permission to enable them to carry out their job role. Access and permissions to the charity's systems and databases holding personal data are regularly reviewed.

INDIVIDUALS' RIGHTS

Under the UK GDPR, individuals have several rights. We have a team of dedicated data protection specialists, and clear processes to handle all rights requests in a consistent manner within the required timescales. These rights can be exercised via our web-form or by contacting Customer Services.

MISUSE OF THE CHARITY PERSONAL DATA

Misuse of the charity's Personal Data is the use of that data in ways it wasn't intended for. We collect employee and members' Personal Data for specific purposes and uses, which are set out in our privacy notices. Misuse of any of the charity's Personal Data violates these requirements. Individuals using any the charity-held Personal Data are never permitted to use this data for their own purposes and must always follow official policy, processes, and procedures in relation to that data.

The charity has zero tolerance of misuse of data, and any individual who accesses the charity's Personal Data for their own purposes will be subject to disciplinary action and mandatory reporting to the Information Commissioner's (IC).

DATA PROTECTION BY DESIGN AND DATA PROTECTION BY DEFAULT

We have procedures and guidance to ensure that high risk processing activities are undertaken considering data protection by design and by default through the entire data life cycle. Data privacy is an integral part of the design of any product, project, processing

activity, system, or service we offer. We implement appropriate measures to assess and protect Personal Data.

PSEUDONYMISATION AND ANONYMISATION

Where appropriate, we use pseudonymisation (a way of processing a person's data without revealing their real identity) to further protect the charity's Personal Data. Truly and irreversibly anonymised data are not subject to data protection law.

AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING (ADM)

The charity does not currently make use of automated decision-making processing activities.

DIRECT MARKETING

Prior consent from data subjects (individuals) is required before sending any electronic direct marketing communications (for example, by email, text, social media direct messaging or automated calls). We have procedures to ensure the requirements of the PECR and data protection legislation are met. The PECR does not apply to non-electronic marketing (postal marketing) but our postal marketing activities do still meet with UK data protection law requirements.

RECORD KEEPING

The charity keeps a record of its data processing activities (ROPA) to meet the requirements of Article 30.

TRAINING AND AUDIT

All the charity personnel have undergone adequate data protection awareness to enable them to comply with data privacy laws. We regularly review our provisions and test our systems and processes to keep information relevant and up to date.

PRIVACY NOTICES

We provide privacy notices on our websites, and employee intranet, in line with the requirements of the UK GDPR and provide the necessary communications to new members, volunteers and employees; we make available any changes that are made to these notices.

ENGAGEMENT OF DATA PROCESSORS

The charity only use data processors that provide sufficient guarantees to ensure that the requirements of UK data protection laws and the rights of individuals are met. Arrangements with data processors are documented in UK GDPR compliant contracts..

SHARING PERSONAL DATA

Sharing of Personal Data with third parties is only carried out where we have a lawful basis to do so, and when relevant safeguards and contractual arrangements have been put in place.

TRANSFERS OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

Personal Data is not transferred outside the UK and the European Economic Area unless adequate safeguards, as set out in Article 46, are put in place and are assessed by the data protection team before the transfer takes place.

BREACH NOTIFICATION

We record and investigate all data breaches and near misses reported to us. All breaches are reported via our breach reporting webform. We have breach management processes for responding to breaches and to help decide whether they should be reported to the IC and data subjects.

ACCOUNTABILITIES, RESPONSIBILITIES, AND GOVERNANCE

The charity's Board: The Board of trustees has ultimate responsibility for the charity's risk management, including setting risk culture and its implementation.. The Board sets risk appetite and delegates authority for risk management..

Data Governance Group: The Data Governance Group is made up of senior staff and the DPO, and is responsible for considering pertinent data protection matters, for making recommendations to the Board and implementing those recommendations.

Data Protection Officer: The data protection officer is primarily responsible for monitoring and assessing the charity's compliance with data protection laws, providing advice, and making recommendations to improve compliance. The charity's DPO can be contacted by email at admin@meassociation.org.uk

POLICY UPDATES

This Policy is reviewed annually, and we will make any updates deemed necessary.

Last updated
13/03/2026 Neil Riley