



## MS Society Data Protection Policy

Purpose:	The purpose of this policy is to enable the MS Society to: <ul style="list-style-type: none"><li>• comply with the law in respect of the data it holds about individuals</li><li>• follow good practice</li><li>• protect the MS Society's supporters, staff, volunteers and other individuals</li><li>• protect the organisation from the consequences of a breach of its responsibilities</li></ul>
Region:	UK-wide
Scope:	All staff and volunteers
Lead Officer:	Claire Stevenson, Data Governance Manager and DPO
Responsible Director:	Vicky Annis, Executive Director of Corporate Services
Key Consultation:	Clare Horwood, Executive Director of Income and Engagement
Approver	Board of Trustees
Committee review	Audit, Risk and Finance Committee
Last Approval	December 2021
Approval Cycle	3 years
Next Approval	December 2024 or at point of legislative change if earlier

### Introduction

#### 1. Purpose and scope

The MS Society is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data and ensuring the confidentiality and integrity of personal data held by the organisation. It will at all times fulfil data protection requirements placed on it by law, and will in particular ensure the individual's right to privacy.

The policy applies to all staff and volunteers, and to others who may be given access to personal data processed by the MS Society.

The purpose of this policy is to enable the MS Society to:

- comply with the law in respect of the data it holds about individuals

- follow good practice
- protect the MS Society's supporters, staff, volunteers and other individuals
- protect the organisation from the consequences of a breach of its responsibilities

All staff must be informed by HR of the contents of the MS Society Data Protection Policy, participate in the required training and take responsibility for implementing the policy. Unauthorised access to or disclosure of personal data, deliberately or through negligence, may be treated as a disciplinary matter.

The MS Society has identified several significant risks, which this policy is designed to address. These risks include:

- putting the data subject at risk as a result of breach of sensitive and/or key personal data
- reputational damage to the MS Society
- potential loss of trust from key supporters
- non-compliance with relevant legislations with reputational and financial (fines) consequences

The purpose of the UK GDPR and the Data Protection Act 2018 are to protect the rights and privacy of individuals, and to ensure that data about them are not processed without their knowledge, wherever possible. The legislation covers personal data relating to identifiable, living individuals, and defines a category of special category (sensitive) personal data which is subject to more stringent conditions on their processing than other personal data. All our working relationships with service users, people affected by MS, staff, volunteers and all information is kept secure and processed in line with the General Data Protection Regulation (GDPR).

## 2. Definitions

### **Data**

Information that is being processed electronically or paper records that are stored in a relevant filing system, where specific information about a specific individual is readily available (not notebooks or bundles of papers).

### **Data controller**

The organisation responsible for how and why personal data is used.

### **Data owners**

Those members of staff who have responsibility for the maintenance and security of named data sets.

### **Data processor**

An organisation which processes data under the instruction of, or in provision of a service to, a data controller.

### **Data Protection Officer**

The member of staff within an organisation with responsibility for ensuring that personal data is processed lawfully in compliance with the statutory responsibilities laid down. The Board has appointed the Data Governance Manager as the MS Society's Data Protection Officer.

### **Data Subject**

An individual about whom personal data is processed.

### **Personal data**

Information about a living individual who is identifiable from the data held on them by a data controller. This may include, but is not limited to, contact details of individuals, donor information, health information, and support provided to people affected by MS and staff and volunteer records.

### **Processing**

Any use of personal data, including obtaining, storing, disclosing or destroying it.

### **Sensitive or Special Category personal data**

Types of personal data which is afforded greater protection in law and has to be treated with particular care. This includes information relating to an individual's physical or mental health or condition, sexual life, religion or ethnicity, trade union membership and genetic or biometric information. Information about an individual's commission or alleged commission of any offence is also subject to additional processing limitations.

## **3. Policy statement**

It is the policy of the MS Society that:

- Personal data shall be processed fairly and lawfully
- Personal data shall only be obtained for specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive to the purpose(s) for which they are processed
- Personal data shall be kept accurate and up to date
- Personal data shall not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of the data subjects
- Personal data shall be protected from unauthorised and unlawful processing and against accidental loss or destruction or damage by appropriate technical and organisational controls
- Personal data shall not be transferred to a country or territory outside the EEA unless an adequate level of protection of the rights and freedoms of the data subject(s) can be guaranteed

## **4. Policy principles**

In order to ensure the policy is adhered to, the MS Society will apply the following principles to all areas of its work:

- Be transparent about its processing of personal data and ensure that individuals have access to their rights as data subjects.
- Avoid causing harm to individuals. In the main, this means:
  - keeping information securely in the right hands
  - holding good quality information, and
  - being fair in the way we use personal data
- Hold Information that is secure, adequate, relevant and not excessive, whether it is kept electronically or in hard copy. In order to achieve this principle the information must be:
  - accurate,
  - kept up to date,
  - obtained and used only for specified and lawful purposes which have been made known to the relevant individuals, and
  - not kept longer than is necessary
- Whenever data on individuals is collected, they will be informed of the intended use of the data, and referred to the MS Society's Privacy Policy. Details of their consent, when applicable, must be recorded.
- Endeavour to inform individuals about whom we hold data whenever we make a significant change to our Privacy Policy.
- Record all personal data processing activities within a central register. This will list the purpose, lawful basis, and third party data processor and data retention period for each processing activity. Where sets of activities are uniform across all or part of the MS Society, they can be registered under one entry.
- Carry out a Data Privacy Impact Assessment on high risk processing activities
- Carry out a Legitimate Interest Assessments on new processing activities based upon Legitimate Interests
- Refresh consent from time to time (as determined by the Executive Group) where processing takes place on the lawful basis of consent
- Seek the agreement of the Data Protection Officer to transfer personal data to third parties (whether as a joint data controller, a data processor, or on any other basis). The Data Protection Officer oversees an adequacy assessment of the transfer and make a judgement based upon the lawfulness of the requests, and the best interests of the individual and others.
- Document all data protection decisions
- Make staff and relevant volunteers aware of their data protection responsibilities and deliver appropriate learning

## 5. Responsibilities and Reporting

Data owners must:

- Ensure that the policy principles are applied at all time on their data sets.
- Ensure that data is recorded accurately and consistently and, where appropriate, with the consent of the individual for the use(s) stated.
- Ensure that the restrictions on use and access to the data are documented and are observed.
- Ensure that the data is secure, and to notify the MS Society Data Protection Officer of data incidents
- Ensure that data which is no longer required is destroyed and that retention periods are observed.
- Ensure that requests for disclosure of data by individuals are given to the MS Society Data Protection Officer soon as received.
- Ensure that the privacy rights of any staff member, volunteer, supporter or third party are not compromised when disclosing data to an individual.
- Personal data is transmitted both internally and externally by approved secure methods.
- Process only the minimum amount of personal data required for the task. (Data minimisation)

## 6. Other relevant policies

- Privacy Notice
- Information Security Policy
- Data Incident Management Procedure
- Comments, Compliments and Complaints policy
- Public Records policy
- Document Retention policy

This policy is owned by:  
Claire Stevenson, Data Governance Manager

Next review date: December 2024 or at legislative change if sooner

## Version Control

VERSION	STATUS	ISSUE DATE	AUTHOR
1.0	Final for issue	Nov 2011	
2.0	Text amended	Oct 2015	G Day
2.1	Final for issue	Nov 2015	G Day
3.0	Reviewed	Nov 2016	G Day
3.1	No changes	Nov 2016	G Day
4.0	Text amended	July 2017	G Day
4.1	Final for issue	Aug 2017	G Day
5.0	Text amended	May 2018	C Stevenson
5.1	Text amended	October 2018	C Stevenson
5.2	Text amended	November 2021	C Stevenson