A6: Handling data

In this section

1. The General Data Protection Regulation
2. Your personal data responsibilities
3. The rules for sending, receiving, storing and sharing emails
4. Using membership data
5. What about images and stories?
6. How long should I keep personal data?
7. Sharing data with third parties

1. The General Data Protection Regulation

All MS Society volunteers and staff must follow the General Data Protection Regulation (GDPR). The GDPR gives people broader rights, and places greater obligations on organisations that control or process personal data than the Data Protection Act (1998), which it replaces. Our obligations apply to personal data held in any form, both electronic and on paper.

We are all responsible for protecting the privacy of individuals and their right to control the ways we use their personal information. We have a detailed Data Protection Policy and Privacy Notice in place to ensure we fulfil our legal data protection requirements, and protect you from personal liability, provided that you follow our guidance.

Data Governance Team

Our Data Governance Team is here to make sure we all meet our personal data, information handling and record keeping obligations. Contact the Data Governance Team for help with any data compliance questions you may have.

Data Governance Team
datagovernance@mssociety.org.uk
Tel: 0203 872 8735

1.1. Types of personal data

'Data' or 'personal information' means a piece or pieces of information which can identify a living person. We hold personal data about our members, supporters, volunteers, staff, and people who use our services.

Examples of personal data include someone's name, address and date of birth, as well as 'special category' personal data which is more sensitive, such as physical and mental health (for example, whether a person has multiple sclerosis), ethnic origin, religious and political beliefs, sexual orientation and trade union membership.

1.2. Why data protection is important

We are a 'data controller' and 'processor', and we have a Register of Processing Activities which documents the breadth of processing we do. We have one registration to cover the whole organisation, including all local processing activities.

Organisations that are data controllers are legally required to ensure that personal data is:

- Fairly, transparently and lawfully processed
- Processed only for specified purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Not kept for longer than is necessary
- Kept secure (both technically and procedurally)
- Not transferred outside of the EU without adequate protection

What is data processing?

Data processing includes anything we do to or with personal information, such as filing, updating, copying, checking and sharing. Data processing also covers simply storing data, even if nothing is done with it.

1.3. Rights of the individual

People have the right to:

- Be provided with privacy information whenever data is collected, which tells them about that processing.
- See what personal information an organisation holds about them, for what purpose, on what lawful basis, where in came from, who it will be shared with, and how long it is expected to be held for.
- Have errors or inaccuracies in their personal information corrected.
- Have excessive or irrelevant personal information deleted.
- Be forgotten – that is, to have all data held about them deleted (in most cases).
- Object to processing.
- Not have solely automated decisions made about them based on their data.

1.4. Subject access requests and other data subject rights

A 'subject access request' is when an individual contacts an organisation to find out what personal information is held about them. You may also receive other types of data subject requests that relate to the additional rights listed above. All subject access requests must be directed to the Data Governance Team.

Your group must not attempt to deal with subject access requests or any other data subject request. You may be contacted by the Data Governance Team if they receive a subject access request or other data subject request.

If asked by the Data Governance Team, you must provide copies of the personal information held by your group about the individual who has made the request.

Privacy statements

Whenever you collect personal data from an individual, you must give them a summary of how their personal information will be processed, and for what purposes.

We do this by including our up to date 'privacy statement' and a link to our full Privacy Notice in all forms we use to collect personal data. This information must be in the same font size as the main body of text.

See Privacy Statements on our volunteer website, or ask the Supporter Care Team for help.

1.5. Your access to personal data

You may have access to personal data as part of your volunteer role. This could include any of the following:

Members

You may be in a volunteer role that is authorised to request membership data to communicate with our members:

- Group Coordinator
- Administration Volunteer
- Lead Support Volunteer
- Finance Volunteer
- Communications Volunteer
- Support Volunteer

Group Coordinator responsibilities

Your Group Coordinator is responsible for ensuring that all volunteers with access to personal data as part of their volunteer role understand their obligation to handle data in line with the GDPR.

Depending on your role, this may mean completing our Data Protection for GDPR eLearning (see 'Using membership data' below) or confirming that you have read and can apply the rules in this section of the Group Handbook.

Volunteers

Your role may include maintaining the records we keep about other volunteers in your group:

- Group Coordinator
- Lead Support Volunteer
- Activities Organiser
- Health and Safety Volunteer
- Fundraising Volunteer
- Transport Volunteer

Service users

You may be in a volunteer role that involves collecting personal data on an exercise class or property register, a minibus emergency contact list or grant application form:

- Activities Organiser
- Volunteer Driver
- Lead Support Volunteer
- Property Volunteer
- Activities Volunteer
- Passenger Assistant
- Support Volunteer
- Information Events Volunteer

Supporters

You may collect personal data about our supporters on sponsor forms or Gift Aid declaration forms, or deal with communications from supporters:

- Communications Volunteer
- Fundraising Events Volunteer
- Shop Volunteer
- Fundraising Volunteer
- Administration Volunteer

See C1: Volunteering with us for guidance on recruiting, supporting and recognising your volunteers.

2. Your personal data responsibilities

We must all take responsibility for ensuring that all personal data we have access to is kept safe and secure, and only used for the purpose/s agreed by the individual. It is crucial that we handle it carefully according to the principles of the GDPR.

2.1. Data protection rules

- All personal data belongs to the person to whom it refers. They have a legal right to see what personal information is held about them.

- Anybody who stops volunteering with us must return all personal data owned by the MS Society to your Coordinating Team within seven days. This includes paper based personal data and personal data held on a computer, laptop, tablet, smartphone, or on an encrypted memory stick (see 'Keeping personal data safe and secure' below).

  Failure to return personal data within this timescale is data theft and may result in the matter being reported to the Information Commissioner's Office (ICO) and the Police.

- You must not publish a person's personal data anywhere unless you have their prior consent in writing for the publication you intend to make. If in doubt, contact our Data Governance Team for assistance.

- You must be discreet with personal information at all times, and maintain confidentiality where necessary.

Safeguarding, emergencies and data protection

You must report all abuse or suspected abuse to the Safeguarding Responders Group, even if you have not been able to obtain permission.

If someone's life is in immediate danger, data protection laws do not prevent you from acting immediately to share information with the emergency services, health professionals or other authorities.

However, if your group is approached by the Police or any other authority asking for information about a person in anything other than a life or death situation, you must always refer them to our Data Governance Team.

See our Safeguarding Policy and guidance on the volunteer website, or contact the Safeguarding Responders Group for help.

2.2. Keeping personal data safe and secure

The GDPR applies to both paper and electronically stored personal data and you must ensure that both are kept safe and secure at all times.

When not in use, all personal data must be stored securely. Only volunteers in roles that are allowed to use personal data must be permitted access to it.

Paper based records

Paper based personal data must be kept in a locked drawer, filing cabinet or cupboard at all times when it is not being used. Access to the key or combination lock must be limited only to volunteers in roles that are allowed to use MS Society personal data. You must not allow members of your family to access personal data you hold.

Avoid taking paper copies of personal data from your home. Where this is unavoidable (such as for events or meetings), you must keep them in your possession at all times. You must not view them where members of the public may be able to see them, and you must never leave them unattended on a train seat or in a car.

Purchasing storage

Providing the necessary equipment for your volunteers to keep data securely is an appropriate use of group funds. If your group doesn't have a lockable drawer, filing cabinet or cupboard, your Coordinating Team should purchase one from a local stationer or website.

When a volunteer leaves, we expect them to return the personal data they hold and any items purchased by your group to store it.

See C3: Your Coordinating Team for guidance on how your group should operate.

Electronic records

Electronically stored personal data must be held in a password protected file on a computer, laptop, tablet, smartphone or on an encrypted memory stick. All devices used to store or access personal data must need a password to be accessed. Access to the device and password must be limited only to volunteers in roles that are allowed to use MS Society personal data.

For guidance on password protection, see IT Support on our volunteer website, or ask the Supporter Care Team for help.

Keeping information in the Cloud

With the exception of MS Society email accounts accessed via Office 365, you must not use cloud based storage (for example, Dropbox, Google Docs or Google Drive) to store personal information and data.

2.3. What is a data breach and what do I do if it happens?

A 'data breach' is any situation where personal data is made insecure. In some situations it will be obvious that personal information has been accessed in error, but this is not always the case.

A breach might be caused by:

- Clicking on unsafe links in emails that breach the security of your computer. This may then give access to your contact lists and may also allow corruption to or damage of data stored.

- Sending an email to a list of contacts using the 'To' field instead of the 'Bcc' field (thereby sharing everyone's email addresses with everyone else, which they may not have consented to, or be happy with). Further unauthorised sharing can happen if that email is then forwarded.

- Leaving personal information in a public place – either in printed form or on a public or shared PC or smartphone.

- Verbally sharing personal information with someone who should not have access to it.

- A mistake in how an IT system is set up.

- Someone else breaking into or 'hacking' an IT system.

- Theft or loss of hardware that contained personal information

This list may not include every possibility of a breach, so if you are unsure, you must speak to our Data Governance Team without delay.

Reporting a data breach

You must speak to our Data Governance Team to report any potential data breach immediately. We are required to inform the Information Commissioner's Office of a breach within 72 hours of any volunteer or member of staff becoming aware of it.

Data Governance Team
datagovernance@mssociety.org.uk
Tel: 0203 872 8735

Reporting a lost or stolen mobile device containing MS Society data

As soon as you become aware that your device is missing, contact IT Lab (our IT support service) to inform them. They will initiate a partial wipe to remove all MS Society data and reset your MS Society email password with you.

IT Lab
Tel: 0207 030 3999

3. The rules for sending, receiving, storing and sharing emails

Under the GDPR, there are specific rules for dealing with emails.

To request your individual MS Society email account, log in or get support, see Using MS Society Email on our volunteer website, or ask the Supporter Care Team for help.

- You must use MS Society email whenever you handle personal data by email, act as an account signatory on your group's cash pooling account, or communicate with external organisations or people by email on our behalf.

- When emailing more than one person, you must not disclose their email address to others receiving the email. Always use 'blind carbon copy' (bcc) when you send emails so that recipients can't see each other's email addresses.

- When emailing members, you must use up to date membership data. A member can contact us at any time to change their email preferences. You must use the Portal to download membership data each time you need it, and delete this as soon as it has been used.

- You must store written and digital communications securely and never share them with third parties. You can only share an email with another MS Society volunteer if you need their help to reply to it.

- You must not use a person's email address to communicate with them unless they have agreed to receive emails from us. If a non-member or local supporter emails your group, this does not mean you can use their email address to contact them about other matters.

- You must offer people the option to opt out of receiving written and digital information from us. Your MS Society email automatic signature includes an unsubscribe option.

  When you receive an unsubscribe request from a member, you must update the Portal or inform our Supporter Care Team.

4. Using membership data

If your group handles money and delivers services and activities, you need to be able to communicate with MS Society members in the area who have agreed for their details to be shared with you.

4.1. Who can access membership data?

You can only access membership data if you are in a volunteer role that is authorised to do so. This is to ensure that we meet our data protection requirements.

Volunteer roles with access to membership data:

- Group Coordinator
- Administration Volunteer
- Lead Support Volunteer
- Finance Volunteer
- Communications Volunteer
- Support Volunteer

4.2. Data on the Portal

Your group must use the Portal to access membership data. This will ensure that we only use up to date information about members who have agreed to be contacted by us.

Each time you use the Portal to download membership data as an Excel spreadsheet or PDF, you will be asked to confirm the reason for the download. You must not use this downloaded data for any other purpose.

You will be prompted to protect the file with a password. You must not share this file password with anyone who is not in an authorised volunteer role.

To request your Portal account, log in or get support, see Using the Portal on our volunteer website, or ask the Supporter Care Team for help.

Data Protection for GDPR eLearning

Both our organisation and individuals are at risk of significant fines from the ICO if we can't show them data protection training records for our staff and volunteers.

Data Protection for GDPR eLearning aims to build your confidence and helps you to avoid making a mistake inadvertently. You can check your learning and ensure your training record is entered by completing the multiple choice test at the end.

You must complete Data Protection for GDPR eLearning if any of the following apply to you:

- Your role involves handling personal information, such as a Group Coordinator or Finance Volunteer
- You have access to membership data
- You use MS Society email, our Portal or Online Recruitment
- Your role specific Welcome and Induction Checklist includes Data Protection for GDPR eLearning as 'must do' training

We will ask you to complete Data Protection for GDPR eLearning even if you have completed previous data protection training.

Contact our Data Governance Team if you have any questions about Data Protection for GDPR eLearning.

4.3. The importance of using current membership data

When sending out newsletters or email communications to members, you must not use membership data that:

- is more than 28 days old
- was requested for a different purpose

Emails and newsletters are classed as marketing and members have the right to change their 'marketing contact preferences' at any point.

If a member requests a change to their marketing contact preferences, you must let the Supporter Care Team know as soon as possible, to enable us to update our membership database within the required 28 day notification period.

If a person does not appear on a current membership list you download from the Portal, you must not contact them for any reason.

5. What about images and stories?

The GDPR applies to images and stories (often called 'case studies') too, although there are some circumstances where it is not necessary to obtain consent for images.

5.1. Images and stories used in advertising, publicity, newsletters and websites

In cases where a person's image or story is intended to be, or may be used publicly, that person's consent must be obtained in writing and kept on file until one year after the last use of the image or story. You must specify to the person how their image or story may be used.

Download a Consent Form from our volunteer website, or ask the Supporter Care Team to send you a printed copy.

Web to Print and our data requirements

Web to Print is an online tool to support our groups to design and produce quality newsletters, stationery, and promotional items. It includes a bank of images with consent forms already on file. You can use these images with confidence that they meet our data requirements.

See B2: Using our brand for more on Web to Print.

5.2. When written consent is not needed

You do not need written consent when taking photographs of crowds or large groups at meetings or similar events. However, it is good practice to let those pictured know why photos are being taken, so that anyone who doesn't want to be pictured can make themselves known.

If a person is seen close up, and can be easily identified, they must give written consent.

6. How long should we keep personal data?

The GDPR requires us to keep data for no longer than is necessary. You must follow these rules for different types of data:

Membership data

Membership data must be downloaded from the Portal and not held locally other than for the time it takes to complete a mailing or other task.

See C4: Membership administration for our membership data rules.

Volunteer application forms

We don't expect your group to hold personal information about potential volunteers. If a candidate who submitted a paper application form is successful, either email or post it to our Supporter Care Team. If you don't recruit them, you must destroy their application form.

See C1: Volunteering with us for guidance on recruiting volunteers.

Health and safety documents

You must post or email Accident and Incident Report Forms to our Health and Safety Team and destroy all copies.

Health and safety documents such as Physical Activity Readiness Questionnaires (PARQ) must be reviewed annually and kept for three years after a person stops taking part in a service.

See A5: Health, safety and wellbeing for more on our risk management system.

Financial data

Our Online Accounting system enables you to safely store financial data relating to individuals. You must retain any other financial data for seven years to meet HMRC requirements.

See B4: Managing your finances for using Online Accounting to store financial data.

Grants

If your group awards grants, you must hold grants information for seven years following the issue of a successful grant application. Unsuccessful applications must be destroyed one year after the decision was made.

MS Support

We don't expect Lead/Support Volunteers to hold personal information about people using your MS Support service, or make case notes about enquiries you have taken, and you must not do so.

See D1: Offering MS Support for more on handling sensitive personal information.

Events

You must retain personal information such as attendance lists and routine correspondence with individuals about events for one year following the event.

See B6: Planning and delivering quality services and activities for how to meet our local priorities.

Stories and photos

Stories and photos must be stored and used for no longer than three years. You must keep the Consent Form for the full duration of use plus another year after the deletion of the stories and photos themselves.

See B1: Availability, contact and communication for our guidance on using case studies and images.

6.1. Deleting information securely

Paper records must be shredded or burnt when no longer needed. Electronic records must be deleted from your PC or device's storage, and the 'recycling bin' must be emptied.

When it's time to replace IT equipment and phones, or you wish to pass them on to someone else, you should reformat disks to ensure that all content is deleted.

7. Sharing data with third parties

If your group provides services and activities, you may need to share personal information about the people who use them with a service provider. We have two processes to support you to keep data safe when sharing it.

You must contact your Local Networks Officer (LNO) before sharing personal information with a service provider not covered below.

For contact details for your LNO, see Your Local Networks Team on our volunteer website, or ask the Supporter Care Team for help.

Service Level Agreements

If your group receives complementary therapies, exercise, physiotherapy and talking therapies from a service provider, whether this is an individual

or organisation, we expect you to set up a Service Level Agreement (SLA) which sets out the expectations of everyone involved.

For SLA templates and frequently asked questions, see Service Level Agreements on our volunteer website, or ask your LNO for help.

This SLA requires your service provider to look after data appropriately. You must involve your LNO if you plan to develop any service or activity that requires an SLA.

Data Protection Undertakings

If your group regularly hires transport or a venue, your service provider must complete a Third Party Data Protection Undertaking Form. This outlines our confidentiality and record-keeping requirements when handling personal information we share.

Download a Third Party Data Protection Undertaking Form from our volunteer website, or ask the Supporter Care Team to send you a printed copy.

Print two copies and ask your service provider to sign both. Give your service provider one copy for their reference and securely store the other copy until a year after you stop providing the service.

> You don't need to obtain a Data Protection Undertaking for one-off taxi, restaurant and hotel bookings.

Group Handbook A6: Handling data v3.3	
Content Owner:	Data Governance Manager
Editor:	Volunteer Resources Editor
Sign off:	Head of Local Networks
Sign off date:	October 2019
Review date:	October 2020