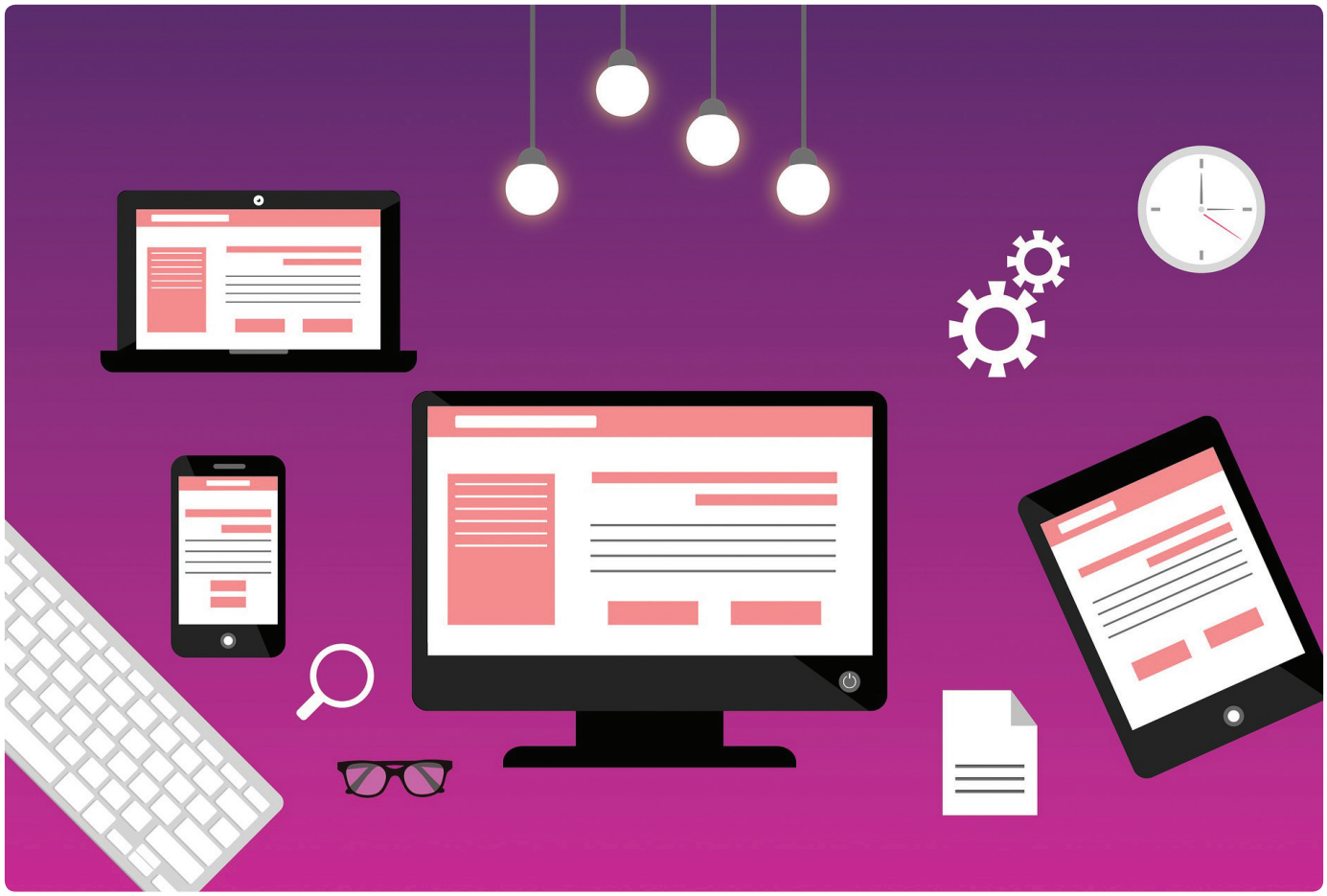
MS Society

Data and Technology Special

May 2018

Teamspirit



Contents

Message from Michelle Mitchell, MS Society Chief Executive

Welcome to this Data and Technology Special Edition of Teamspirit.

As many of you will know, the General Data Protection Regulation (GDPR) comes in to effect on 25 May. We've been doing lots of work across the organisation to prepare and ensure that we're compliant with the new legislation. This special edition of Teamspirit is designed to support you; providing information in one place so that you feel prepared and know how best to handle and process the data your group holds.

I know that the GDPR may seem like a daunting (possibly admin heavy) prospect, but its basic principle is hugely important. The legislation stems from the Human Rights Act, with the core principle to "protect the fundamental rights and freedoms of individuals". This is something that we, at the MS Society, believe and champion. This principle is the starting point for all our decisions and processes implementing the GDPR.

The legislation is complex, but it's useful to think of it in terms of what you think an organisation should be allowed to do with your data, especially sensitive data such as a connection to MS. If we're thinking like that, we're half way there!

This special edition goes beyond compliance with the GDPR and touches on other areas of data and technology. We're making great strides forward in modernising how we do things to be more efficient and to reach and support more people living with MS. Fantastic examples of this in our groups are the introduction and recent improvements to the Portal, Online Recruitment and Accounting Online, and of course our new website! We'll continue to build on this. Developing how we use and exploit data and technology in the coming years is essential to ensure we continue to have a real, positive impact in an ever-changing modern environment. Thank you for your continued commitment and efforts taking on new challenges and learning different ways of doing things.

I really hope this will be a useful resource for you. Please note, you don't need to know or understand the GDPR in depth. We'll provide all the guidance needed to support you in your role.

Thank you again for everything you do in our MS community. I'm always filled with admiration by the incredible care and support our groups provide. If you have any questions or concerns please get in touch with your LNO or our Data Governance team, who will be happy to answer your questions.

M. Mitchell

The legal bit

The legislation

As a volunteer **you don't need to know the GDPR legislation** in detail, or to develop policies or other resources specifically for your group. But here's a bit more information, in case you're interested.

The GDPR is a new Europe-wide data law which will replace the Data Protection Act (DPA) on 25 May 2018. UK organisations will still have to meet GDPR standards post-Brexit.

The GDPR builds on the same principles as the DPA, but goes further by:

- giving individuals whose data is held more rights
- requiring organisations be more accountable and transparent about what they do with people's data

The MS Society also has to comply with The Privacy and Electronic Communications Regulations 2003 (PECR) which regulates consent around how organisations communicate certain messages by phone and email. This is particularly relevant to our fundraising activities.

The principles

GDPR is a principles-based piece of legislation not a prescriptive way of working; it's the MS Society's responsibility to satisfy ourselves that the principles are being appropriately applied and to evidence how we meet them if we get investigated by the Information Commissioner's Office (ICO).

These principles state that personal data must be:

1. processed lawfully, fairly and transparently
2. collected and used only for specified reasons, and must not be used for other incompatible reasons
3. kept to the minimum required
4. accurate and kept up to date
5. kept for no longer than necessary
6. kept securely – using processes and IT to prevent breaches

We all need to keep these principles in mind and follow them when processing personal data.

We'll refer to these throughout this edition of Teamspirit, highlighting where and how they can be applied to the activities you do involving personal data.

And remember...

You don't need to know the GDPR legislation in detail.
There's lots of support and guidance available:

- Our Group Handbook has been updated with a new section on data handling, covering all GDPR requirements. See page 14 for more information on this.
- There's new e-learning, appropriate to your role. See page 15.
- A GDPR FAQ is available at volunteering.mssociety.org.uk/GDPR-FAQ
- And, of course, this edition of Teamspirit!
  You can find a handy 'jargon buster' on page 16 for your reference.

Storing, transferring and disposing of data

Top Tip: **Remember the data protection principles:** do you really need this data? Are you only using the data for the purpose you collect it for? And, delete it as soon as that purpose has ended.

Personal data

Personal data is any information which enables the identification of a living person. For example, their name, address, date of birth, and banking details. The GDPR recognises that some data is particularly sensitive. Information about a person's health (including their MS status), sexuality, ethnicity, religion, political beliefs, or trade union affiliation is all 'special category' data under the GDPR and has additional protection.

Data processing is simply **anything we do** to personal data, e.g. checking it, giving it to a supplier, or using it to get an understanding of who our members are. Processing is also **anything we don't do** to personal data. Just by storing someone's information in a filing cabinet or computer we're processing their personal data. And the GDPR applies to all of this data processing.

Fair processing

People have a right to understand how their data is used and why. For this reason, whenever you ask for personal information from members or non-members you need to provide them with the relevant privacy statement, available at volunteers.mssociety.org.uk/privacy-statements These explain how we process data, and gives all the information we need to provide.

Transferring data: safe use of email

Email is not a secure way of communicating, so we need to be careful in how we use it. Incorrect use of email by local groups is the most common cause of low-level data breaches at the MS Society. We know that accidental breaches are easily done, but they're avoidable with a few simple steps...

- **Use the official MS Society email account**

Groups should use their MS Society email account. This also reassures recipients that your message is authentic. If your group is not already using your group account find out how to get started at volunteers.mssociety.org.uk/MS-Society-email

- **Use 'bcc' not 'to'**

When sending out emails to more than one member or other contacts, e.g. a newsletter, you must put all recipient addresses in the 'bcc' field, not the 'to' field. This means no one but the sender sees the addresses of recipients. If you don't, everyone sees each other's email addresses, and we don't have permission to share email addresses in this way. The only email address which should go in the 'to' field is your group's own email address.

- **Password protect personal information**

If you need to send personal data by email don't type or paste information into the email

message. Attach the information as a document or spreadsheet. This file must then be password protected before sending. You should then share the password with the recipient through a different means of communication e.g. by text or over the phone.

Groups should, where possible, use MS Society provided Microsoft Office 365, for all software needs, and for sharing information with other volunteers.

Sharing data with someone else (volunteers, suppliers and third parties)

In certain situations your group will need to provide information about members with someone else (either volunteer, supplier or third party) so that they can provide a service. For example, for:

- regular transport or room/ facility hire
- providers of physical therapy and classes

Before sharing personal data with a supplier, you should check that a Service Level Agreement (SLA) is in place. SLAs require suppliers to look after data appropriately and must be in place before sharing personal data with a supplier.

Keep the information you share to a minimum. For each piece of information provided to a volunteer, supplier or third party consider whether this is necessary for them to provide their service.

You don't need to obtain an SLA for one-off taxi, restaurant and hotel bookings although the person who's data you are sharing must be aware you are doing so.

Make sure the SLA is kept securely; somewhere you can access it should you need to.

You can read more about third parties on pg. 14 of the GDPR FAQs.

Storing data safely

There are certain situations when your group will need to store personal information locally, for example when processing a grant or organising an event. Keep in mind the Data Protection Principles, particularly that data should be kept: to the minimum required, no longer than necessary and securely.

If the data is printed, keep it in a locked filing cabinet which only specified people have access to. You may like to use group funds to buy a lockable filing cabinet, if you don't have one.

If it's held electronically consider:

- having a password on the device and/or file
- If possible encrypt the hard drive of the computer you're using (you may want to search "Bitlocker" on the internet to investigate this further).
- Backup – ensure you always have a recent copy of the personal data. Regularly save a copy either on an encrypted external hard drive or encrypted USB. If you use a USB to store or transfer data you must first encrypt it (you can find instructions online at online-tech-tips.com/computer-tips/encrypt-usb-flash-drive/)
- If possible don't use cloud based storage or back-up, for example Dropbox. If you do use cloud based storage or back-up, you'll need to verify the security of these services, and that storing data in this way doesn't constitute a data breach. We strongly recommend you use the large storage providers (eg Amazon, Google and Microsoft) and consider the GDPR principles as you select a provider including whether the information is held within EEA.

Storing, transferring and disposing of data

How long to keep data for

It's important not to keep personal data for longer than necessary.
Please follow these timeframes for how long to keep personal data you process:

Document/ data type	Retention period
Membership details and contact list	Download from the Portal for each use and delete afterwards
Grants and related information	7 years following payment for a successful grant application; 1 year after decision for an unsuccessful grant application
Personal stories and images (originals)	5 years from consent
Personal stories and images consent forms	6 years from consent (ie. for 1 year after last possible use)
Newsletters (which may include personal stories and images)	Retain for as long as useful. No delete-by requirement
Member/ contact health-related information	Hold only for as long as required e.g. until the event or session for which processing of the data was required
Volunteer contact details	Delete when volunteer leaves
SLAs	6 years after last use of supplier

Deleting data

Try to remember to delete expired data as soon as it has passed its retention period end, as outlined in the table. You may wish to use a spreadsheet and/ or simply note retention dates within the document itself to help manage this.

To manage the deletions, we strongly recommend that you have a "spring clean" once a year to check all the data you hold, and delete/ destroy expired files.

For digital records, remember to empty the trash can/ recycle bin to delete the item.
For printed documents, shred before placing in the recycling, or safely burn papers.

Storing, transferring and disposing of data

Keeping volunteer data up to date

When a new volunteer starts, please make sure they fill out a volunteer application form, which can be found at volunteers.mssociety.org.uk/resources/volunteer-application-form This includes a statement about how we'll keep information. The form should then be securely sent, via email or post to Supporter Care so your new volunteer can be added to the Portal. If this form is sent via email, the paper form must be destroyed afterwards.

If you change your details or see something out of date on the Portal, you should either contact Supporter Care or fill out our update contact details form: volunteers.mssociety.org.uk/news/2017/10/update-your-contact-information

All new volunteers will be signposted to the eLearning before they handle any data as part of their role. This is detailed in the relevant Welcome and induction checklist so please make sure you're giving all your new volunteers theirs.

When a volunteer decides to leave their role, please make sure to follow the 'exit process'. This process intends to:

- make sure they know their time and commitment has been appreciated
- provide the opportunity to give us feedback on volunteering with us
- and crucially, that the leaving volunteer no longer has access to our online tools and other systems. You can find out more at volunteers.mssociety.org.uk/when-volunteer-leaves

Rights for individuals

1. Objecting to processing

Everyone has the right to object to us processing their data. Sometimes this will simply be to opt out of receiving communications. To make sure we're giving people the option to object you must include the follow text in the same type size as the rest of the document at the base of all group mailings: **To unsubscribe, please reply to this message stating 'unsubscribe'.**

You must act promptly on all unsubscribe/opt-out requests by forwarding them to Supporter Care so that they can update our records.

2. Right to be forgotten

The GDPR gives a new right for individuals' records to be completely deleted. This process can be more complicated than it might at first appear, and there are some situations where the right doesn't apply, so if your group receives such a request please contact Supporter Care to deal with it.

3. Corrections

Individuals have the right to have mistakes in their data corrected quickly. If you receive a message from a member or contact noting that their information is inaccurate please inform Supporter Care as soon as possible.

4. Access

People have the right to access the vast majority of information which organisations hold about them. There are, however, some situations where all information shouldn't be provided, for example where personal information about another person would also be revealed. If your group receives such an access request please contact the Data Governance team.

All contacts referred to throughout this publication can be found on page 15.

Apps, tool and systems

The Portal

The Portal is your data source

Every time you need contact details or a distribution list, you should download these from the Portal, your online source for up to date membership lists. The data you download should be used for the intended purpose and then deleted once your task is completed. Next time you need a distribution list or contact details, download a new up-to-date copy.

Having copies of contact information and holding on to old lists could mean you don't have up-to-date information including the individual's wishes on how their data should be used. It could also increase the risk of data breaches. Downloading a new list from the Portal every time is safer and helps make sure we're contacting people according to their current preferences.

Members receive newsletters and information about events, campaigns and related information from their local group. When an individual's contact details appear on the Portal the group may communicate with this member. If they don't appear on the Portal list they must not be communicated with.

For contacts who aren't members, groups must obtain the individual's consent to receive regular communications. We know that many groups have, up until now, held non-members' data locally but with the GDPR we'll need to store this more securely.

We're expanding the Portal so that all the contact details you hold – both members and non-members – can be stored in it. We can't send organisation-wide or group communications to any non-members who have not given consent and are therefore not on the Portal. Being stored on the Portal means the data will be more safe and secure, and should be easier for you as everything will be in one place. You will be able to do this from the end of May. Please contact SSadminhelpdesk@mssociety.org.uk / 0203 828 6861 for more information.

Our MS Society website

Our fantastic new website is a great source of resources and information. It has a refreshed design with improved navigation, search function and structure. And it's mobile and tablet friendly.

Online Recruitment

Our latest online tool, Online Recruitment, enables you to advertise vacancies on external websites as well as our own volunteering opportunities web page. You can use it to manage the entire recruitment process online, from tailoring your advertisement and promoting your vacancy, to confirming a successful candidate in a role.

To set up your Online Recruitment account, log in or get support, visit volunteers.mssociety.org.uk/online-recruitment on our volunteer website, or get in touch with the Volunteering team.

Social media guidance

Social media enables people to interact with each other by both sharing and consuming information over the internet. Many of our groups and volunteers use social media to share news stories, images and information about MS and what we do. Your Coordinating team may decide to set up a group account or you may use your own personal account.

Local volunteers participating on our Policy Guidance Panel have helped develop our new guide on using social media. This can be found

Apps, tool and systems

on the volunteer website at volunteers.org.uk/socialmedia#safety It guides you through the social media policy and offers support and information on how to represent us on social media. You can also find information on how to keep your data safe online.

If you have any ideas or suggestions for additional help that you or your Coordinating team would like to get the best out of social media for your group, please send them to volunteering@mssociety.org.uk with 'social media suggestions' as the subject line.

Apps and tools

There are lots of apps that you may find interesting and useful in your volunteering role. Here's a list of some of them; what they do and what we liked/didn't like.

Please remember that all the data protection principles still apply when you use these tools (and you may need to issue privacy statements before using them) and some will have a cost or licence requirements that need to be considered.

Trello

An online tool that provides a visual layout for projects and ideas. Everything is set out in lists on boards and each list is made up of a card that can be filled with information, documents, pictures and videos.

- Once you understand the framework, it's so easy, and it seems as though the possibilities are endless – great for organising your life!
- Unless well structured, the information and cards can become overwhelming.

Slack

Slack brings all your communication together in one place. Its real-time messaging, archiving and search are great for teams.

- This is great for team chats. It's so easy to use, even for beginners. It's great to be able to create a separate chat for topics.
- It can become a distraction if people overuse it.

WhatsApp

WhatsApp is a messaging system between selected groups of people and has voice calling as well. With the option to notify you when you receive a message, just like receiving an SMS (text message).

- Great way to have a private conversation with selected people. Practically eliminates the need for a texting and calling plan.
- Tied to a single device and phone number.

Goanimate

Let's you tell your story in animated videos. Upload your videos and pictures to use your own images and logos.

- Platform quite easy to use, no animation or design skills are needed to get going and there is a great library of templates and characters.
- The free trial is great but beyond that it can get expensive – be careful of the payment plans/schedules.

Smartsheets

An intuitive online project management and collaboration tool. It has a spreadsheet like interface, coupled with file sharing and workflow.

- Easy to share spreadsheets with teams and the ability to access the information from any device (laptop, phone, tablet) and from anywhere. Excel files import seamlessly.
- When compared to Excel, some of the functionality isn't quite as good e.g. graphs and multiple tabs.

Apps, tool and systems

Zoom

Video conferencing and online training system. Provides video, audio and screen-sharing.

Easy to share spreadsheets, Powerpoints and Word documents with teams and the ability to access the meeting from any device (laptop, phone, tablet) and from anywhere. Excel files import seamlessly.

The free version only permits 40 minute meetings which may not be enough for your needs. The full version has a license fee but your local team has a license, so speak to your LNO for more information. The recording function has significant data protection ramifications and should not be used without gaining consent from every attendee. We therefore strongly recommend not recording.

If you are already using any of these apps, or other digital tools, we'd love to hear what you think, and share it with other groups. Please let the Volunteering team know at volunteering@mssociety.org.uk

Staying safe from fraud online

Some quick tips to help keep you safe online:

1. Never follow a link in an unexpected email – it's also a good idea to check the spelling of the URL (website address) to make sure it's legitimate. For example, amaz0n.co.uk is incorrect and shouldn't be accessed.
2. Never give your personal or payment details, or online account information online or over the phone – unless it is to a verifiable and trusted source.
3. Chances are, any offer you receive out of the blue is likely to be very risky or a scam including offers to "review investment, banking arrangements or pensions". Do your own research and check every offer out.
4. Don't allow your (or the MS Society's) bank account to be used to move money for others. Be vigilant and query any money in your bank account that you don't recognise and only pay for legitimate expenses, invoices and costs.
5. Make your password strong. A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music"). If you want to be doubly certain just change the odd letter to a digit (for example, "I l0v3 c0untry music")
6. When in doubt, throw it out. Links in emails, posts and texts are often how cybercriminals try to steal your information or infect your devices.

Computers and other devices

Top Tip: Good, well maintained systems, computers and mobile devices help secure data.

Buying and setting up a computer

Buying a computer can be a confusing task with lots of acronyms. Here's a quick guide to what some of them mean and some basic advice on what to go for:

Processor: There are two main manufacturers: intel and amd. For general word processing and web surfing you don't need a powerful one, so the lower range Intel Celeron, Pentium or i3 should suffice.

RAM: If you are running Windows 10 then you need at least 4Gb, but it will run faster with 8Gb. Google chrome books will work with 2Gb, but 4Gb is better.

Hard drive: These come in two types; SSD (new and *much* faster, but generally low in storage space) and HDD (older and *much* slower, but you get more storage space for the price). If you have lots of music, photos and videos that you need to store then you may need to stick with the HDD, but if at all possible go with the new SSD - ~250Gb will be fine for most.

Operating system: This is what runs when you turn the computer on. There are four main ones, Windows 10, Windows 10 Pro, Apple Mac OSX and Google Chrome OS. The only one of these that *can't* be made really secure (encrypted) is Windows 10. If possible get one of the others.

Once you've got the computer, it needs setting up. You should create different usernames and passwords for each of the people that are going to be accessing it, and don't make anyone but yourself the administrator. Turn on the systems extra security features (encryption) to protect the data and never leave the password written down near or on the computer – if you do need to write it down ensure it is kept well away from the computers and is in a locked drawer.

Keeping your smartphones and tablets safe

Mobile phones and tablets are an essential part of our lives including the role we play with the MS Society, with increasing amounts of data being stored on them. As they're mobile, they need even more protection than desktop computers. With this in mind, here are our five quick tips to help keep your mobile phone and tablet safe:

1. **Switch on password protection**
   A good PIN or password will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to lock your device, without the need for a password. However, these features are not always enabled when you first receive your device, so you should always check they have been switched on.
2. **Make sure lost or stolen devices can be tracked, locked or wiped**
   The majority of devices include free web-based tools that are invaluable should you lose your device. They can help you track the location of a device and remotely lock access, erase data or retrieve a backup of data stored on the device. You can set up your devices to a standard configuration with a single click.

Computers and other devices

3. **Keep your device up to date**
   All manufactures (for example Windows, Android, Apple) release regular updates that contain critical security fixes to keep the device protected. This process is quick, easy, and free. Devices should be set to automatically update, where possible. At some point, manufacturers will discontinue their support for older devices, at which point you should consider replacing them with a newer model or version otherwise your data may not be secure.
4. **Keep your apps up to date**
   Just like the device, all applications that you have installed should be updated regularly. These updates will not only add new features, but will also fix any security issues that have been discovered.
5. **Don't connect to unknown Wi-Fi Hotspots**
   When you use public Wi-Fi hotspots (for examples in hotels, coffee shops or public transport) there is no easy way to find out who controls the hotspot or to be assured it's secure. If you do connect to these hotspots, somebody else could access what you're working on and potentially your login details of apps, systems and documents. The simplest precaution is to not connect to the Internet using unknown hotspots and instead use your mobile 3G or 4G mobile network. You can also use 'tethering' (where your other devices such as laptops share the data connection from your phone) or a wireless 'dongle'.

Disposing of computers, smartphones and tablets

Before disposing of any old computer make sure you've copied any data (documents, spreadsheets, pictures etc.) that you need to keep onto your new computer/ laptop/ tablet.

Once this is done you can delete these files from the old device, and empty the recycle bin. However doing this doesn't actually delete the files from the hard drive of the old computer and they can still be accessed.

To ensure the data can't be retrieved you can download and run a free disk eraser tool such as Eraser or Darik's Boot And Nuke which can be found through searching on Google. These should be downloaded to and run from a USB drive, as you can't wipe the hard drive that you install them on.

Once you've deleted the data ensure you either donate, or recycle the device responsibly. Some local councils have Waste Electrical and Electronic Equipment (WEEE) collections points at their recycling centres which can be found through searching on Google.

When things go wrong

Top Tip: "Tell it all, Tell it Fast, Tell the Truth"

Data breaches

We know that errors and accidents with data can happen. If you lose data or there's a breach, don't worry – our Data Governance team is here to protect you individually and the MS Society from prosecution and fines. But they can only do this if they're informed immediately.

If you suspect a loss of data may have taken place contact the Data Governance team immediately to report your concern on 0203 872 8735. Even if you think you've caused the potential breach, it's important that you report it as soon as possible so that the team can assess the risk and advise on the best course of action.

A loss of data or 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. Some examples of what could cause a breach are:

- Clicking on unsafe links in emails
- Sending an email to a list of contacts using the 'To' field instead of 'Bcc'
- Leaving personal information in a public place – either in printed form or on a public or shared PC or smartphone
- Someone breaking into or 'hacking' an IT system
- Sending communication with personal details to the wrong recipient
- Theft/loss of a computer, or mobile phone that contained personal information

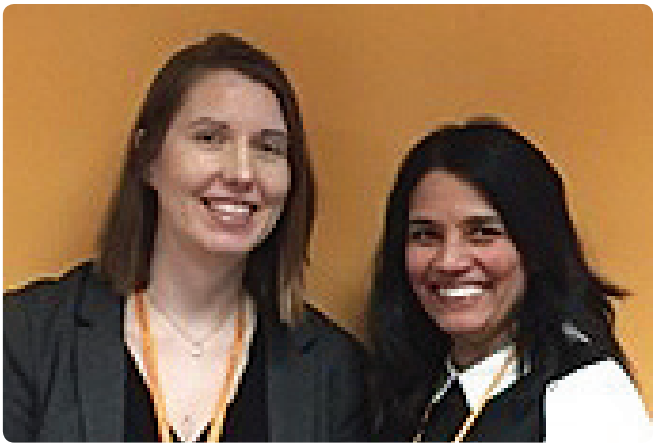
Fines and penalties

The MS Society believes and champions the rights of individuals, therefore we're committed to protecting people's data. As well as our moral obligation, there are also financial implications if we fail to protect personal data. The Information Commissioner's Office (ICO) has powers to investigate, stop processing and impose fines. Under GDPR, the ICO has increased powers to fine up to 20m euros for serious breaches and individuals can also bring compensation claims against organisations.

Please don't think the ICO will be lenient on the MS Society because we're a charity – they have already stated that they expect charities to uphold the same standards and have fined charities under the existing DPA!

More help

The Data Governance team



Claire and Michelle

We're a new (ish) team put together in 2017 to help the MS Society meet the challenges of the GDPR, and we've been working hard on the GDPR for the last eight months! Looking forward, our broader role is to move towards better data governance and providing support for staff and volunteers, ensuring that the data we hold is accessible to those who need it and respects the privacy rights of individuals.

Here's a little about the people behind Data Governance:

Claire is the Data Governance Manager and comes from a compliance and records management role at a University. In her spare time she helps to lead a running club for people who've spent most of their adult lives on the sofa. The best part is replacing the calories burnt with post-run cake! Claire is also the proud mum of one little boy and three rescue greyhounds.

Michelle is the Data Governance Officer and her background is governance in a small health charity. Alongside supporting Claire on the GDPR projects and being the appointed team blogger, she spends her spare time upcycling unwanted items, gardening and playing football (very badly) with her eight year old son.

We know that data protection can be confusing, but we're here to help. Please do get in touch if you have any questions.

The Group Handbook

The Group Handbook will always reflect key requirements, and the online tools and processes for groups to use.

We've fully updated our data handling guidance, including new information about recognising data breaches, storing, sharing and destroying data. Throughout the handbook, we'll make it clear how the GDPR impacts on your activities.

We've also updated:

Online tools
Learn more about how Online Recruitment can help your group find new volunteers. Find out how the information you add to the Portal about your services and activities is now automatically published on our website.

This updated Group Handbook is available at volunteers.mssociety.org.uk/group-handbook for you to download the sections you need.

More help

New data protection eLearning

Top Tip: Complete the Data Protection eLearning module as soon as possible – it will be 30 minutes well spent!

With a new law comes new training! We've updated our eLearning to help you make the change. The Data Protection for GDPR eLearning is for both staff and volunteers and aims to build confidence around the GDPR and ensure we're compliant, and not inadvertently making mistakes.

The eLearning is mandatory for Group Coordinators, Finance Volunteers and anyone else who has access to data – such as Support Volunteers, or those who have access to systems including the Portal, MSS email and Online Recruitment, or who regularly post on social media for the group. Even if you've only recently completed the Data Protection Essentials course, you'll need to complete the new course to update your knowledge.

If you're carrying out one of the listed roles, tasks or have completed the eLearning previously, you'll receive an automated email with a link to the new eLearning. These will be emailed out in batches from early June and will include information about how to access the course.

It's vital that you complete this eLearning as soon as you can. Both the organisation and individuals are at risk of significant fines from ICO if we can't show them training records for both staff and volunteers. The eLearning must be completed by 25 May 2019.

If you'd like to feedback on what further support and resources you need, we'd love to hear from you – please contact the Volunteering team.

Key contacts and resources

Contacts:

Data Governance
datagovernance@mssociety.org.uk

Supporter Care
supportercare@mssociety.org.uk
0300 500 8084
Supporter Care, MS National Centre (MSNC)
372 Edgware Road, London NW2 6ND

Volunteering team
volunteering@mssociety.org.uk

Services and Support Admin
ssadminhelpdesk@mssociety.org.uk
0203 828 6861

Find your LNO: volunteers.mssociety.org.uk/local-networks-team

Resources:

The GDPR FAQ
volunteers.mssociety.org.uk/GDPR-FAQ

Group Handbook
volunteers.mssociety.org.uk/group-handbook

Health and Safety
volunteers.mssociety.org.uk/health-and-safety

More help

Jargon Buster

Consent – Permission from the individual to process their data, given provision of information about the processing in a privacy statement.

Contractual legal basis – The legal reason for processing personal data for a necessary purpose, such as entering into a contract (e.g. employment contract).

Data controller – An organisation which determines the purpose for which, and the manner in which, any personal data is processed.

Data processor – An organisation that carries out processing on behalf of a Data Controller.

Data subject – An individual whose information is processed.

Explicit consent (to process special category personal data) – consent where an explicit action, such as ticking an unchecked box accompanied by an affirmative statement, along with information explaining what giving consent means.

GDPR – General Data Protection Regulation

ICO – Information Commissioner's Office – the organisation responsible to the government for enforcing information compliance in the UK.

Legal basis – One of the six means by which data processing is lawful under the GDPR.

Legal obligation – Legal basis for processing personal data arising from necessity to process personal data due to a legal obligation (e.g. PAYE return to HMRC).

Legitimate interest – A legal activity in the MS Society's interests which is fair to, and respects, the rights of the individual.

Information Commissioner – The government regulator responsible for enforcing data protection law in the UK.

Personal data – Information from which a living person can be identified, including data where it is necessary to consult other data that MSS has access to in order to identify the individual.

Privacy statement – A statement accessible to the individual at the point of data collection which notes the identity of the Data Controller, the purpose(s) for processing the data, who information may be shared with, and how long information will be retained for.

Processing – Anything which is done with personal data by an organisation. This includes passively holding the information as well as transferring the information, checking, recording, disclosing etc.

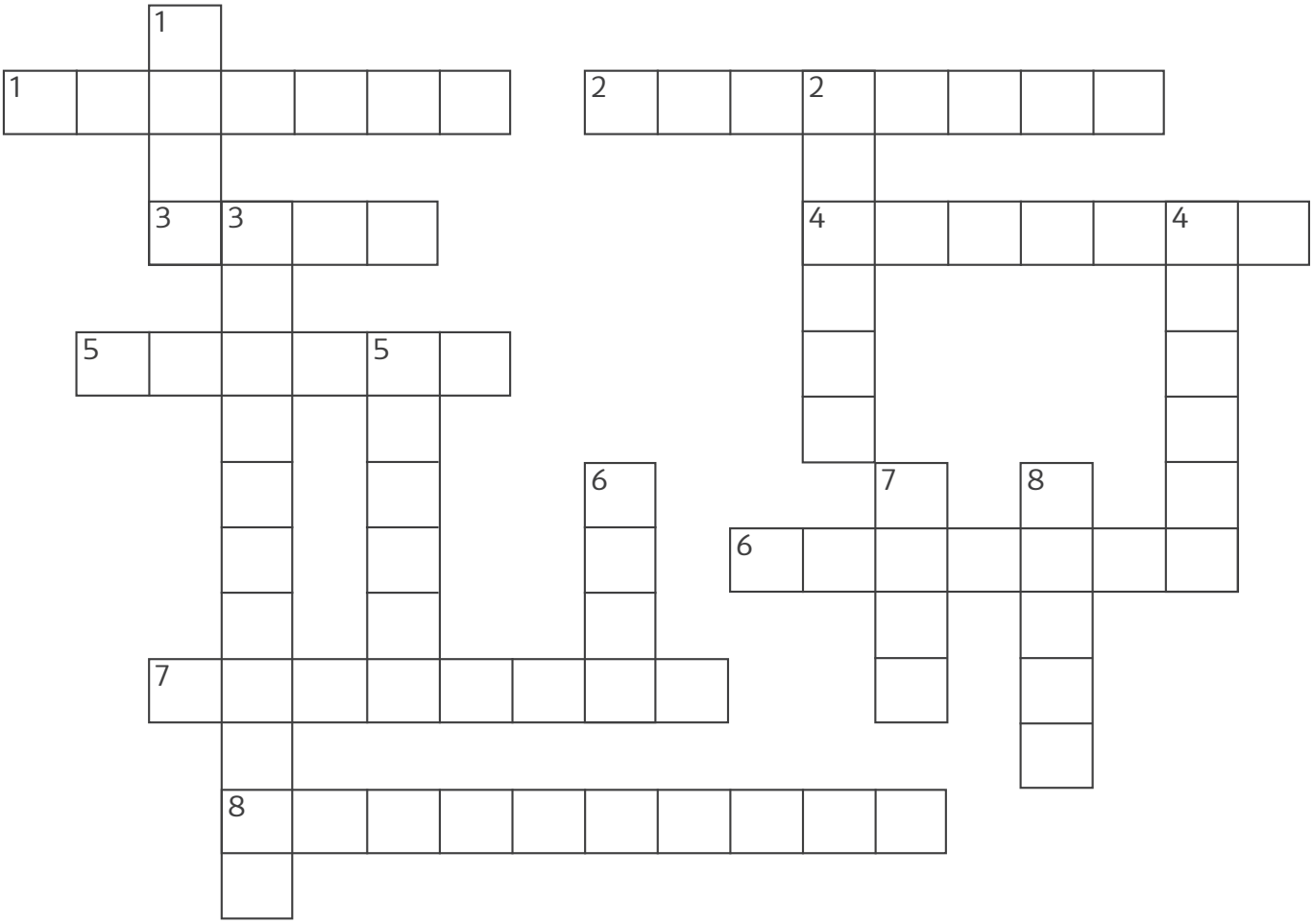
Special category personal data – Sensitive information about a living, identifiable individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation.

Vital interests – Legal basis for processing personal data arising from life and death situation (e.g. providing medical information to emergency services when an individual is incapable of consenting.

Some fun

Try our data and information crossword

Answers available at:
volunteers.mssociety.org.uk/teamspirit-data-and-technology-special-crossword-answers



Across

1. Keep from danger or defend from attack
2. Acts of breaking or failing to observe a law
3. It may be crunched
4. Acceptance without protest
5. Impervious to break-ins
6. A state in which one is not observed or disturbed
7. "Open Sesame"
8. Able to be defended with logic or justification

Down

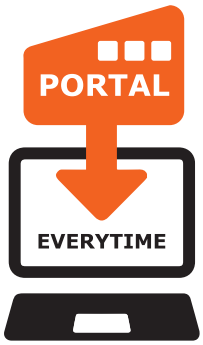
1. Thesaurus entry
2. The opportunity to approach or enter
3. A leader or organisation must be
4. Call to a state of preparedness
5. Entitlement
6. Free from bias
7. Not OK from a GDPR perspective
8. Foundation of an argument

Our GDPR key messages

Always use bcc when emailing multiple people

Lock it before you leave it: computers, devices and paper containing personal data should always be kept in locked storage when not in use

Password protect all files containing personal information



Download a membership list from the Portal every time you do a mailing and delete the list afterwards

All email communications should be made using your official MS Society email account

Data breaches: tell the Data Governance team immediately – we have 72 hours to report a breach to the ICO

Give a privacy statement every time you ask for someone's data – forms are available on the volunteer website

Data collection should be kept to a minimum

And always remember the six data protection principles.