**Data Handling Guidance**

**What is GDPR and what does it mean for local networks?**  
GDPR is an important change in government legislation regarding data protection. It stands for The General Data Protection Regulation. It effectively provides an update to the Data Protection Act – bringing in new requirements and increasing the penalties for breaches. It comes into force on 25 May 2018. It’s not a cliff edge so there will be ongoing compliance activities post May. However, it’s important that we have the core building blocks in place by 25 May 2018.

**Does this apply to our local network?**  
Yes, Parkinson’s UK is the ‘data controller’. The local groups support the ‘data controller’ by owning their local information assets, for example, membership or mailing list/database.

**My local group is only a small one with a few members. Does this still apply to me?**  
Although the risk is lower, if you collect and store any personal data – like names and addresses – you will have to manage the data in accordance with strong data protection principles.

**What are the key things to consider for local groups?**  
The principles of data protection that we already work with still exist under GDPR. All local groups need to ensure that any personal data is:

* processed securely
* updated regularly and accurately
* limited to what the local group needs
* used only for the purpose for which it is collected
* only used for marketing purposes if the individual has given the local group consent to do so

**What is a Privacy Notice?**  
Under GDPR, you will need to tell people about how and what you do with their data at the point you collect it. An overarching Privacy Notice is now available on the Parkinson’s UK website. A bespoke Privacy Notice for local groups is available to download from our website. Hard copies will also be available for local groups.

If your local group has a website, you should make sure there is a link on your site connecting to the Parkinson’s UK Privacy Notice on the main charity website. Please also make sure that you upload the bespoke privacy notice to your own website

**What are ‘Individual Rights’ under GDPR and how do we respond?**  
Under GDPR, there are enhanced rights for individuals. If you are contacted by anyone to enact any of the below rights, please contact the data protection officer at [dataprotection@parkinsons.org,uk](mailto:dataprotection@parkinsons.org,uk)

* The right to be informed about the processing of your personal information
* The right to have your personal information corrected if it is inaccurate and to have incomplete personal information completed
* The right to object to processing of your personal information
* The right to restrict processing of your personal information
* The right to have your personal information erased (the ‘right to be forgotten’)
* The right to request access to your personal information and to obtain information about how we process it
* The right to move, copy or transfer your personal information (‘data portability’)
* Rights in relation to automated decision making, which has a legal effect or otherwise significantly affects you

**How do we respond if someone submits a subject access request?**  
Subject access requests (requests for copies of personal data from individuals) will now need to be responded to within one calendar month. If anyone submits a request for their personal data, please notify the data protection officer immediately who will co-ordinate the response.

**What are the obligations of third parties?**  
This may mean that if you use any third parties to process data, for example hosting your website, then we must have a written contract in place. The data protection officer will be liaising with website hosting partners that are used by most local groups.

**What are our responsibilities for data retention?**  
Retention policies need to be clear. Parkinson’s UK will issue a data retention policy and guidance. You can’t keep data for longer than is necessary for the purpose it was collected. You also need to inform people how long you will keep their personal data for and you can’t keep it indefinitely. For example, a member may not have renewed for a couple of years – how likely is it that they will return? If the answer is ‘unlikely’ then their core data should be deleted.

**What is****privacy by design?**  
It means building data protection controls into new processes or systems from the outset. If you are planning any new processing activity which is high risk to personal data, please contact the data protection officer who can advise whether a privacy impact assessment is required or not.

**What do I need to do if there is a** **data breach?**  
If you are aware of a data breach, please contact the data protection officer as soon as possible. As a charity, we will only have 72 hours from being aware of a breach to report it to the Information Commissioner’s Office if it meets the threshold criteria for reporting to the regulator. This will be decided by the data protection officer. For example, if a membership secretary holds the membership data on their laptop and it gets stolen, the data is now at risk and a breach would have to be reported.

You need to make sure that personal data is held securely, for example, electronic documents are encrypted, and password protected and backed up on a regular basis, and any paper records are stored in a locked container.

**What if we process children’s data?**  
There are additional protections for children’s personal data. If you collect children’s personal data, then you need to liaise with the data protection officer for further advice.

**What are our data transfer obligations?**   
One of the principles of GDPR is that you can only process data for the purpose it is collected. This means if you collect a name and contact details of an individual, so that they can become a member of your group, you can’t simply use that information to allow other bodies to contact them for marketing purposes. You also need to tell people when they join your group if you are going to transfer their data, for example, to Parkinson’s UK or external organisations.

**Does all this only apply to data that is held digitally, for example, on a computer, or does it cover paper records too?**  
This may be a good opportunity to review filing systems and to limit the amount of paperwork you manage. Personal data collected manually and stored in files as a hard copy still has to be managed in accordance with the data protection regulations.

As you can imagine, some of the legislation is more difficult to implement in relation to paper copies. Paper documents can get into the wrong hands easily and this could easily become a data breach. One small slip and it’s too late. For example, an individual leaves sensitive paperwork on a train, a courier loses an archive box full of payment records, a lead volunteer has files stolen from their car. These are all real-life situations where paper documents can fall into the wrong hands. All paper records of personal data must be stored in a locked container.

**My local group keeps its membership records ‘in the Cloud’ (for example, via shared files on Dropbox or Google Drive), what should I do about that data?**  
Data security is key, and when storing anything online, you need to protect yourself by keeping passwords safe and ensure files that contain personal data are encrypted. Dropbox, OneDrive and Google Drive have built in security measures for the protection of files while in storage – or in the process of being shared. We are currently looking at the requirements for a secure system that could accommodate volunteers’ processing activities in the future.

**What about former committee members?**When someone leaves the committee/group who has processed personal data in the past, it is important that paper records/emails that have gone beyond their retention period are deleted/shredded.

**What about e-newsletters?**Some local groups have, or will have an e-newsletter that people subscribe to – opted in to receive – via their website.

The subscriber list is held in the website hosting. People self-manage their subscription and can unsubscribe at any time. The website hosting partner used will be reviewed by the data protection officer.

**Publishing email addresses**It’s recommended not to publish email addresses on your local website unless they are already in the public domain and you have received specific permission to publish the details yourselves (for example, from your Parkinson’s nurse and your Parkinson’s UK local adviser).

**What can I do locally to enhance cyber security?**In a typical ‘phishing attack’, scammers send fake emails to thousands of people, asking for sensitive information (such as bank details) or contain links to bad websites. They might try to trick you into sending money, steal your details to sell on or they may have political or ideological motives for accessing your information. Phishing emails are getting harder to spot, and some will still get past even the most observant users. We can’t eliminate all risk but what we can do is raise awareness.

* If you’re using your home laptop/PC, please ensure the virus software is up to date and active.
* Be suspicious of emails that are addressed to you generically. For example, Dear customer, are sent from a sender you don’t recognise or come with unsolicited attachments. If you have any concerns, do not open the email and delete it.
* If an email contains a link, hover your mouse over it before clicking on it. The true destination will be displayed without taking you there. If it doesn’t match the sender’s description don’t click on it.
* Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official looking emails by including logos and graphics. Is the design (and quality) what you'd expect from a credible, large organisation?
* Is it addressed to you by name, or does it refer to 'valued customer', 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
* Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
* Look out for emails that appear to come from a high-ranking person within your organisation, such as a trustee or manager, requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
* If it sounds too good to be true, such as a large donation in return for banking details, it probably is. It's most unlikely that someone will want to give you money, or give you access to some secret part of the Internet.
* If you leave your computer or tablet unattended remember to lock it, for example, by pressing the windows key and L.
* If you are getting rid of your computer or tablet or any digital storage such as a USB drive, which has personal data stored on it, this must be properly deleted or the hard drive destroyed before disposal. You can literally do this by removing the drive and smashing it with a hammer.

**Passwords**

* If you don’t have a password to access your home computer, please set one up.
* Make sure your passwords are strong – at least eight characters long, does not contain your name or complete words and include a mix of characters.
* Do not share passwords or use the same passwords multiple times.

**Handling data electronically**

* Make sure that any electronic files that contain personal data are password protected or put somewhere secure so only people that need them can access them.
* Emails, unless they are from one Parkinson’s email address to another Parkinson’s email address, are not secure. They should be thought of as postcards – the contents easily read. Please be particularly thoughtful when sharing information, even with fellow committee members, by email.
* To send information securely, you can password protect MS Office documents.
* If you do share electronic files that contain personal data, by email or on a USB, make sure these are password protected. However, when emailing, don’t include the password in the same email as the data and communicate this separately to the recipient.
* When sending emails to a group of people, make sure to protect each person’s email address by using blind carbon copy (bcc). If you’re not sure how to do this ask your volunteer co-ordinator.
* Make sure all electronic files that contain personal data are properly deleted when no longer needed, for example, deleted from both the hard drive and recycle bin.

**Handling data manually – for example in paper files**

* Make sure any manual files that contain personal data are kept securely, for example, in a locked filing cabinet and are not left lying out unattended.
* If you do share manual files that contain personal data, such as by post or by hand, make sure you take the necessary steps to ensure it arrives safely. For example, keep it in a sealed envelope, consider whether the package will fit through the recipient’s letter box or whether email would be safer.
* If you must send manual files that contain sensitive personal data by post, this must always be sent by recorded delivery or courier.
* Make sure all paper files that contain personal data are securely destroyed when no longer needed. For example, by using a cross cut shredder or by giving them to your volunteer co-ordinator.