PARKINSON'S UK
CHANGE ATTITUDES.
FIND A CURE.
JOIN US.

Volunteer Data Protection Guidance - your questions answered

We've collated some of the most frequently asked questions on Data Protection into one place. You can use the headings below to jump to the section you're interested in, or use CTRL + F to search for a keyword related to the answer you're looking for, for example 'phishing'.

Contents:

Section 1: The basics

1. What is personal data?

Personal data (or personal information) is information that allows you to identify an individual. Personal data includes information about an identifiable individual. Examples are: name, address, date of birth, email address, social media handle, photos and videos. Personal data also includes things like a person's religion, beliefs, health issues and gender identity.

When you collect personal information about an individual you normally use one of these ways:

- You receive it in a data collection form, for example from a new member at your group.
- You take information over the phone or by email.
- You take photographs or video, maybe at a Parkinson's UK event you're volunteering at.

You must keep all data safe for the duration of the activity it has been collected forFor example, if you take forms from one place to another keep them in a secure bag, with a zip or lock.

In order to process someone's personal data you need to have a lawful basis to do so. For example, if they are members of Parkinson's UK and they appear on your membership list, then they have given us consent for their local group to get in touch with them and you may do so.

2. Does data protection law 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.

Parkinson's UK 215 Vauxhall Bridge Road, London SW1V 1EJ
T 020 7931 8080 E enquiries@parkinsons.org.uk W parkinsons.org.uk

3. 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.

Section 2: Collecting data
When you collect personal data, you must make sure it is accurate and up to date. If you allow collected data to become out of date or inaccurate this is a breach of the data protection legislation. If you are collecting data about local group members, you must plan regular data accuracy reviews.

4. What is a Privacy Policy?
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 Policy is now available on the Parkinson's UK website. A bespoke Privacy Policy 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 Policy on the main charity website. Please also make sure that you upload the bespoke privacy policy to your own website

5. How do I collect personal data by phone or in person?
Sometimes you need to collect personal information in person or by phone. Data protection legislation still applies when we collect personal information face-to-face or when speaking on the phone. For example, a Branch Membership secretary might contact a new member on the phone to introduce themselves and find out some information about them.

- When speaking to someone on the phone, you must explain who you are and why you are collecting the personal information.
- Whenever you collect personal information on a form that needs to be uploaded to a membership database, keep it safe until you update your database.
- Remember, be precise. Only ask for what you need and record it. Make clear and concise notes.
- Avoid discussing personal data in places where you may be overheard. If you allow personal information to be disclosed by talking in front of other people, you may cause a data breach.
- Make sure you've collected information accurately. Read it back to the person giving the information, to make sure it's correct.
- Make sure you are sharing personal data with the person you are expecting to share it with. Try to call them, or if they call you, use caller ID to confirm you are talking to the correct person.

6. What about health data?
If you are capturing health data, such as information about someone's Parkinson's diagnosis, you must get the explicit consent of the individual. This data is particularly sensitive so there should be tight security controls using the tips for question 5, above.

7. How do I collect personal data by email and email multiple recipients?
In your volunteer role, you might need to send and receive personal data via email, for example if you're organising for a group of people to attend an exercise class. When sending emails to multiple people do not put all the email addresses in the 'to' field. This would mean everyone will be able to see everybody else's email addresses, which is personal information and a personal data breach.

The ICO has issued updated guidance to organisations when sending emails to multiple recipients. When you use carbon copy, all those in the 'To' field and the 'CC' field can see each other's email addresses. You may use this to inform the recipient that other relevant people are aware of the email.

When you use BCC, all those in the 'BCC' field can't see each other's email addresses. You may use this to copy in someone discretely or send a bulk email with a large mailing list. However, forgetting to use BCC, frequently leads to the accidental disclosure of all the recipients' email addresses.

In one example of the repercussions of failing to BCC an email sent to multiple recipients, the ICO fined a public enquiry £200,000 for failing to 'BCC' an email, thereby identifying possible abuse victims. The fine would nowadays be far higher, following a change in the penalties.

The ICO has asked organisations to use alternatives to the blind carbon copy (BCC) email function when sending emails containing sensitive personal information. Sensitive information may include, but is not limited to, special category information eg health data. Whether information is sensitive can depend on the context and you should consider what impact it would have on people if there was a breach. For example, financial information or information that might be used to commit ID fraud would be sensitive information for these purposes.

While BCC can be a useful function, it's not enough on its own to properly protect people's personal information. If you are sending any sensitive personal information, you should use alternatives to BCC.

Is an email address personal information?
If you are able to identify a living person, whether directly or indirectly, from it, then an email address is personal information.

An email address which clearly relates to a particular person is personal information. For example, if it is in a format such as douglas.smith@gmail.co.uk it will reveal the name of the person who will receive the email. Some email addresses can reveal more information about someone, such as where they work (if it is a corporate email address). Remember that even if email content doesn't have anything sensitive in it, showing which people receive an email could disclose sensitive information about them.

Can we use BCC?

You may use BCC with other measures if the personal information you're sharing isn't sensitive and there's little risk. For example, if you have general information, such as an internal newsletter, and you wish to avoid 'Reply all' responses.

However, it is important to remember that you will often be dealing with sensitive data regarding Parkinson's or newsletters, knowing who has received it may reveal sensitive information about the recipients.

When sending emails to multiple recipients that contain or relate to special category information, you must use other secure methods to send the email other than BCC. For example, using bulk email services eg Mailchimp HubSpot or mail merge. We have provided a list of providers below. Your email service provider should provide further information on how to use mail merge. For example, Google and Microsoft provide support on how to use mail merge.

Example of Bulk email providers

- SendX
- MemberMojo
- ActiveCampaign
- Mailchimp
- Constant Contact
- HubSpot

- When you ask for data over email you must explain who you are and why you are collecting the data.
- Always create a new email. Don't ask for personal data on an existing email chain. When using email to collect personal information, do not then use that email chain for discussing something else.
- Parkinson's UK has to make sure that we do not retain personal data for longer than it is necessary, and this includes any personal information we send or receive via email. Don't keep emails for longer than necessary.
- If you are sending personal data by email you must send the information as an attachment in a password-protected document. It is not to be in the text of the email. You could share the password by calling or texting the individual. Do not include the password in the original email.

8. How do I take photographs or video?

Be aware of member photo preferences.

- You can't use a photograph or video if there is no photographic preference in place.

- Make sure anyone taking photographs or video of activities is aware of the photo permission preferences of the group.
- When taking photographs or video on a personal device make sure you delete any copies of the photos or videos that may have been backed-up automatically to the cloud.
- When you have finished using the photos or video remove/delete them from your device.

9. 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.

Section 3: Using and sharing data

10. How can I use personal data?
When you use personal data, you can only use it for the specific purpose it was collected for. For example, in a volunteer role as a support group contact, you might use personal data to communicate with the group about the arrangements of their next meeting. You shouldn't use it to send them information about wider neurological research or campaigning. Other specific purposes for which you might collect personal data include:

- Contacting people about arrangements for meetings and associated activities.
- Informing members and carers about rules and policies
- Caring for members and administering any medication or emergency treatment.

Unacceptable uses of data includes

- Sharing data with third parties without consent.
- Continuing to use data obtained from members after you have left Parkinson's UK.

11. What about sharing personal data?
Data protection legislation does not prevent the sharing of personal information, but it does regulate it.

The following guidelines will help you share information within the law:
You can share personal information for purposes to administer and manage membership. When you share data, only provide information that is necessary.
You may share personal data without permission if there is imminent risk of harm to a person. This could mean sharing the data with police or other statutory agencies.

12. How should I download personal information?
If you do need to download an electronic list onto a laptop or a tablet, make sure the document is password-protected.

If you print documents you must keep them secure.

Remember also to delete the downloaded copy of the data when it is no longer needed. Check you don't have a duplicate of the data in the downloads folder on your computer. If you share your computer or other device with anyone then you must make sure they cannot access data.

13. 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 the 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.

Section 4: Rights and requests

14. What are the rights on personal data?

Data protection legislation gives individuals a number of rights over the personal data we hold and use about them. These six rights are:

- The right to be provided with copies of the data we hold about them (previously known as a Subject Access Request or SAR).
- The right to have the data we hold about them corrected if they believe it is wrong.
- The right to have the data we hold about them deleted.*
- The right to ask us to temporarily stop using the data we hold about them.*
- The right to question how we use the data we hold about them.*
- The right to be provided with copies of the data we hold about them in a format that can be used by another organisation.*

*These rights have exemptions allowing Parkinson's UK to refuse the request if certain circumstances apply.

15. What type of request might I get?

You might be asked to:

- Provide copies of an individual's data.
- Check or correct an individual's data.
- Delete an individual's data.
- Stop taking an action based on the information we hold about an individual.

Or you may receive requests like these:
'I want to see and be provided with copies of the data you hold about me.' 'The address you have for me is out of date, I want it corrected.'
'I want you to delete my husband/wife's data from your records.'
'Why are you using my data? I haven't given you permission to do that.' 'Why am I getting emails about gifts from your on-line shop?'
'Are you allowed to use my personal information for doing that?'

If you're asked to update address information for example, this can be altered to the rest of the organisation in Assemble, or you can contact our Supporter Care team. If someone asks for their data to be deleted, check with them if they wish their data held in relation to their volunteering, or by the local network to be deleted only, or if it is everything Parkinson's UK holds on them. If it is the latter, these requests should be flagged to the DPO at dataprotection@parkinsons.org.uk Parkinson's UK needs to respond as soon as possible and within 30 days.

16. 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.

Section 5: Data retention

17. 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.

18. 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.

Section 6: Data breaches

19. 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.

Section 7: Consent

20. What is the difference between marketing and service emails?
Service emails contain essential information needed for taking part in Volunteering and Local Networks. These messages can include information about:

- Safeguarding
- Essential training
- Policies and procedures
- Membership information
- Changes in leadership

Marketing communications are all messages which do not fall into essential information. For example, messages that promote the sale of goods, services or organisational ideals and anything that falls outside of essential information.

If it's hard copy communications that you're sending through the post - then no you don't need consent and this could be within the grounds of legitimate interests. However, the postal communications should still indicate how someone can stop receiving the postal communications if they want to.

If an individual is not a member of Parkinson's UK, you must ensure you are capturing their data compliantly using the local consent form which is on our website to download, so you can also send them 'marketing' emails or texts. You should store these completed consent forms locally, they don't need to be sent to a Parkinson's UK Office.

You don't need to have an individual's permission if you have a *need* to contact them - for example they have signed up to a class that is cancelled or having emergency contacts in case there is an urgent safety concern - but must have their consent for general mailings, for example, to send them newsletters.

21. What about unsubscribing from newsletters?
Some local groups have, or will have an e-newsletter that people subscribe to. If a contact requests to unsubscribe from a list, they are exercising their rights as data subjects. It is important that you put a footnote on the newsletter such as the one below to illustrate how someone can withdraw their consent.

You're receiving this email because you have subscribed to the newsletter. If you do not wish to receive further communication like this, please contact the (insert volunteer role that manages the newsletter)

It is important once you receive the unsubscribe request that you remove their details from your newsletter database.

Section 8: Security

22. What if I'm using an electronic device?
You may process personal information on your personal devices such as smartphones and tablets. If copies of data (such as email attachments) are stored on many different devices, there's an increased risk that it'll become out-of-date or inaccurate over time. There's also an increased risk that it'll be retained for longer than necessary because it's difficult to keep track of copies. It is important to

- regularly review and delete the data that is held on devices.
- make sure that devices are password protected
- regularly delete the information on the device if it is no longer needed
- ensure that if the device is lost or stolen, you can remotely locate it and wipe the data
- be aware of automatic updates to cloud storage and delete documents regularly.

23. I've set up an email address to use for my volunteer role; what should I consider when using this?
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. If you have put your email address on the website, there is an increased

risk that you will receive scam emails and phishing attempts. The guidance below will help you deal with these.

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.
- 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.
- It's preferable that any electronic files that contain personal data are stored somewhere secure so only people that need them can access them.
- 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 staff contact
- 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.

24. 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.

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.

- 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

25. 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. Two factor authentication should be set up to protect your account.

26. What can I do locally to respond to unsolicited emails and phishing?

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. 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. 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?
- 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.

PARKINSON'S UK
CHANGE ATTITUDES.
FIND A CURE.
JOIN US.

Appendix 1: IT Security Tips

- Windows computers should be running Windows 10 and be kept updated. Windows 7 is not supported and should not be used online. Ideally, if Windows 10 Professional is installed, BitLocker encryption should be activated.
- Anti-Virus software should be installed and updated. Ideally it should be the full, not free, version.
- If Microsoft Office suite is installed, it should be a version that is supported by Microsoft (Office 2013 or later).
- There should be separate logins if others use the laptop.
- Public WIFI should not be used.

The following home router WIFI guidelines should be followed:

1. Change the default name of your home Wi-Fi

The first step towards a safer home Wi-Fi is to change the SSID (service set identifier). SSID is the network's name. Many manufactures give all their wireless routers a default SSID. In most cases it is the company's name. When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. This gives a hacker a better chance of breaking into your network. It is better to change the network's SSID to something that does not disclose any personal information thereby throwing hackers off their mission.

2. Make your wireless network password unique and strong

Most wireless routers come pre-set with a default password. This default password is easy to guess by hackers, especially if they know the router manufacturer. When selecting a good password for your wireless network, make sure it is at least 20 characters long and includes numbers, letters, and various symbols. This setting will make it difficult for hackers to access your network.

3. Enabling network encryption

Almost all wireless routers come with an encryption feature. By default it is turned off. Turning on your wireless router's encryption setting can help secure your network. Make sure you turn it on immediately after your broadband provider installs the router. Of the many types of encryption available, the most recent and effective is "WPA2."

4. Make sure you have a good firewall

A "firewall" is designed to protect computers from harmful intrusions. Wireless routers generally contain built-in firewalls but are sometimes shipped with the firewall turned off. Be sure to check that the wireless router's firewall is turned on. In case your router doesn't have such a firewall, make sure you install a good firewall solution on your system to watch for malicious access attempts to your wireless network.