Guidelines for data processors

Introduction

For scheme volunteers (this includes anyone within your scheme, from coordinator to walk leader)

This guidance is based around the 6 principles of the GDPR (listed under Appendix A of the guidelines) to ensure that any processing of personal data you undertake as part of your volunteering duties is carried out within the law. As someone who handles personal data on behalf of Ramblers Walking for Health, your role is termed a 'data processor.'

Data protection is everybody's responsibility. As a Walking for Health scheme volunteer, you will process data on behalf of Ramblers Walking for Health, which means you are responsible for looking after other people's data.

If you stop performing a volunteer role, you should inform the Walking for Health national team of any data you have been managing and agree if this should be destroyed or handed over to another volunteer. You must not retain any copies of personal data.

Care should be taken when handling personal data but the approach we require is no more than common sense. For example, do not access personal data on a shared computer in a public library; do not store personal data on more devices than necessary; do not leave printed copies lying around. Do keep your personal devices as secure as possible. More information on keeping data safe and secure is below.

If you are unsure about how you should be managing personal data as part of your role, please contact walkingforhealth@ramblers.org.uk, or your delivery officer.

The walker registration form

Under GDPR, it is essential that personal sensitive data cannot be linked in any way to an individual. An example of personal sensitive data is a person's health information. It is vital that you do not keep a record of a walker's health information (see below, 'special categories of personal data'). The forms must be kept secure at all times (including in a locked cabinet when being stored) and destroyed after the data has been inputted onto the Walking for Health website.

The health survey

The walker registration form also asks walkers for consent to receive a health survey by email requesting further information. This survey is not linked at all to an individual and remains completely anonymous.

For individuals without an email address, paper forms are available that can be given to new walkers. These forms will not contain any information that can link to the identity of the walker. Please do not add their names to the top of the forms. This health data can then be inputted by web and data administrators as normal onto the survey monkey database online, which is **not connected** to the existing database.

Scheme volunteers will be provided with a survey link from their coordinator in order for them to input the health data onto the online survey. Once this is done, the forms must immediately be securely destroyed.

Personal data

The GDPR outlines how personal data can be used. Personal data means any information relating to a living person who can be directly or indirectly identified by that information. As a data processor you should only collect the following.

Personal data includes:

- Name (title, first name and surname)
- Postal address (full or partial e.g. postcode)
- Email address
- Telephone number (home or mobile)

Special categories of personal data

The GDPR also governs the use of sensitive personal data, which is now described as special categories of personal data - and there are stricter controls regulating the collection and use of this information. Sensitive personal data includes ethnicity, race, political affiliation, religion, union membership, health, sexual orientation etc.

Walking for Health scheme volunteers should not be handling special categories or sensitive data at a local level. We have changed the walker registration form to reflect this. However, there may be some exceptions - for example, Incident Report forms which may contain health data.

Data processing

Data processing involves:

- Collecting data
- Recording and holding data (electronically or in paper-based forms)
- Any activity that uses the personal data (such as organising, adapting, changing, retrieving, consulting, disclosing, erasing or destroying the data).

Examples of data processing at a local group or area level for Walking for Health are:

- Updating the Walking for Health database
- Using walkers' personal data to send out your group or area's walk programme
- Filling in an Incident Report form
- Publishing a walks programme which includes walk leaders' names and contact details.

Consent

The walker registration form includes space for walkers to indicate their contact preferences (their 'consent options').

There are several different versions of the walker registration form, to allow schemes to choose the most relevant consent options for walkers. Each scheme coordinator decides which version to use and will be able to provide copies. All volunteers must ensure that data is used appropriately and that a walker's contact preferences ('consent') are respected.

We must all abide by these contact preferences. For example, if a walker has opted out of email and communications, you may not send them any marketing or 'non-core' communications (see below). Regardless of contact preferences, you can always contact walkers about your core activities. Examples of Walking for Health **core** activities:

- Storing administrative data for your volunteers and walkers
- Sending volunteer rotas or instructions
- Letting walkers know that a walk is cancelled
- Changing the meeting point of a walk.

Examples Walking for Health **non-core** activities:

- Sending information about activities your group or area is running, for example socials, walking festivals or other events
- Sending details of local campaigns
- Recruiting volunteers
- Sending annual reports

You can manage walker consent by following our consent guidance. You will only need to do this if you are contacting walkers for non-core activities as listed above.

We have also developed a template for you scheme to use in order to re-consent your walkers.

Keeping data safe and secure

Subject access requests

Under the GDPR, individuals (in our case, the walkers) can request to see all of the data we have about them on record. This is called a "subject access request". If you receive one of these, please do not respond, but notify the Ramblers data protection officer (dataprotectionofficer@ramblers.org.uk) within 24 hours who will advise on next steps.

Tips for keeping personal data safe and secure

Keeping your personal devices secure is one of the best ways to safeguard personal data stored electronically. Here are some simple things to remember to keep your electronic devices and all the data on them, safe:

- **Establish strong passwords and/or passcodes** for all your electronic devices (laptops, personal computers, tablets and smartphones). Where possible, ensure you use a combination of letters and numbers for a hard-to-crack password.
- **Keep laptops secure by using a username and a unique password**. Make sure to never leave your laptop or any device where it is at the risk of being stolen or compromised, for example in a car.
- **Use antivirus protection and anti-malware software**. These serve as the last line of defence against unwanted attack through your network.
- **Update your computer programmes regularly**. Data security is enhanced with every update. Frequently updating your programs keeps you up-to-date on any recent issues or holes that manufacturers and programmers have fixed.
- Enable your device to lock after a short period of time. Most devices do this automatically, so after a set time devices “lock”. This is useful so that your devices are protected if you have to leave your screen for any period.
- **Avoid using public PCs or laptops for official use** as in most cases you are unable to verify the level of anti-virus or online security on the devices.

Paper documents

We recommend that you do not print out personal data or keep paper copies of data, as this is the least secure way to manage data. However, sometimes you may need to. In this case, make sure all physical copies are kept carefully and securely to avoid them being been seen or used by unauthorised people, stolen, tampered with or used for alternative purposes by any third party. To do this, keep data together in a file and ideally out of sight when not in use – for example in a locked cabinet. As soon as the data is no longer needed, securely destroy the data by shredding.

Disposal of data

Storing and archiving data is considered ‘processing’ of personal data, even if the data is not used or updated. Therefore, to comply with GDPR, personal data must be securely disposed of when it is no longer needed.

Electronic data

Electronic data must be completely deleted when it’s no longer needed. If deleting data within a file, delete the data from the file, and then re-save the file. If deleting a whole file containing data delete the file and then go to the Recycling Bin on your computer and delete the file from there too.

Any CDs and/or DVDs containing personal data must be cut up or crushed before being thrown away.

When disposing of old equipment (such as PCs), please be mindful of data security. Some retailers, such as the larger Currys/PC World stores, offer a secure data wiping service for around £35. For those without access to a high street store there is software available online that will overwrite the entire hard drive to remove the data – see https://dban.org/. Devices that don't have removable storage media, such as mobile phones, usually come with a function called something along the lines of 'Restore to factory settings' to wipe the data.

Paper documents

Paper documents should be shredded and put in the bin (not recycling) or disposed of using suitable confidential waste facilities.

Mismanagement of paper documents containing personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, that personal data, is considered a breach under GDPR.

Examples of data breaches include:

- Mobile devices, briefcases and bags stolen from vehicles.
- A website with personal data being hacked.
- Documents with personal data missing after being left unattended.
- Used computers or mobile devices sold without first destroying personal data.
- Lost, unencrypted memory sticks and drives containing sensitive information.

If a breach has occurred, or you are worried one might have, please notify the Ramblers data protection officer (dataprotectionofficer@ramblers.org.uk) **within 24 hours** who will advise on next steps.

Training

We are aware that this is a complex area, and extra training and support may be useful. We will inform you of training opportunities and further guidance as it becomes available. Please look out for further communications.

In the meantime, you can look through our FAQs in the GDPR toolkit.

If you need further help, have questions or concerns; please get in touch with your delivery officer or email WalkingforHealth@ramblers.org.uk.

Appendix A

The six principles of the GDPR are:

1. Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

5. Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Integrity and confidentiality:

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.