6. Data Protection

6.1 Principles of Data Protection

Data protection is about protecting people's privacy. This is the purpose of data protection in any organisation, and is at the heart of data protection law, including the new General Data Protection Regulation (GDPR) that came into force in May 2018. The most important step towards protecting privacy and complying with GDPR is understanding some basic principles. These are:

- Know what personal data is
- Only collect, store or use personal data if your group needs to do so for a clear, specific purpose
- Only collect, store and use the minimum amount of data you need for your purpose. Don't keep extra data if you don't know why you need it, and don't keep data that is no longer needed for a clear purpose
- Make sure people know how to contact you if they want you to remove their data from your records
- Tell people what data you have about them if they ask you to, and remove it if requested
- Store data securely
- Be clear whether data belongs to your group or to you personally. Just because you have access to contact details held by the group, doesn't mean they are your personal contacts.

If you keep these principles in mind, you are likely to be respecting people's privacy and meeting the fundamental requirements of GDPR

6.2 What Data Does Your Group Collect

Personal data is information about a person which is identifiable as being about them. This includes basic things like names and addresses, and also more complex or sensitive information such as ethnicity, criminal record, employment history, sexual orientation, and health information.

Personal data can be held electronically or on paper. Photographic and film images are also considered to be personal data if people are identifiable in them.

Think about what personal data your group holds about people. This is likely to include names and contact details, but may also include other more sensitive information.

It is important to understand whether personal data belongs to a group or to you personally. For very small groups this can be a bit confusing. A good rule of thumb is to consider whether you met a person, or gained their information, in the course of your involvement with the group. If you know someone because of your role in a group, and have only gained the information through the course of running group activities, the data you hold about that person belongs to the group and not to you personally. You should not use it for personal reasons without explicit consent.

You should only collect, store or use personal data if you have a clear purpose for doing so. This means that your group must know *why* you have people's personal data. If there is no longer a purpose for holding someone's data, it should no longer be kept.

To be legal, your group should only collect, keep or use personal data if you are doing so to fulfil a purpose which fits into one of the following lawful bases:

- To serve your group's legitimate interests, or
- Because you have explicit consent from the person whose data it is, or
- To fulfil a contract with the person whose data it is, or
- To meet a legal obligation, or
- To protect someone's life, or
- To perform a public task.

6.3 Privacy Notices

When your group collects personal data, or uses someone's data to contact them, it should be made clear to them why you have their data, what you are using it for, and what their rights are. This means you should provide them with a privacy notice.

A privacy notice is a piece of written information which tells people why you need or have their data. It should include:

- the name of your group;
- what the data will be used for;
- which legal basis you have for using the data;
- how long the data will be kept;
- whether the data will be shared with a third party, including if it will be stored on a third-party website (e.g. in Google Drive or DropBox);
- that individuals can ask to have their data removed at any time, and contact details to use to do this.

If you are collecting and using data on the basis of explicit consent, you should provide a privacy notice when you request the consent. If you are using data without explicit consent, you should provide a privacy notice either when you collect the data or, at the latest, the first time you contact someone. See Appendix E for a sample Privacy Notice that you can augment to your Group's needs.

6.4 Storing Personal Data

Personal data must be stored securely. If your group keeps personal data on a computer, it should be password protected. You should have up-to-date software to protect them from malware and viruses. If you store information on paper, it should be filed securely.

If your group stores personal data on the internet (e.g. attached to emails, in Google Drive, in Dropbox, etc) you should check that the companies storing the data comply with GDPR regulations and that the data is not transferred outside of the EU. Most big companies have privacy policies which confirm they comply. However, email marketing company Mailchimp currently stores data outside of the EU, so it may be simpler to choose a different mailing list provider, which also offers free services to organisations with small mailing lists.

It is important that you know who is storing data on behalf of your group, and that everyone understands the need to keep it secure and up-to-date. It's best to agree a system, and to minimise the number of places you are storing data. Otherwise you can easily lose track of what you have. A simple way to do this is to have one central list of contacts, either on paper, on a computer, or securely stored online, which everyone refers to. It's best to nominate one person to look after the list. In many groups this would be the secretary's job.

Avoid keeping data for the group on an ad-hoc basis in personal phones and address books. If you write down someone's details when you are out and about, add them to the central list and then delete them from your private phone or address book.

Although it is useful to nominate one person to look after personal data for your group, it is very important that you *do not* refer to this person as a "Data Protection Officer". This is because the term "Data Protection Officer" has specific legal meaning, and organisations that have a Data Protection Officer have additional obligations which small groups do not need to worry about.

6.5 Keepining in touch with your Committee

To organise together as a group, the core people involved in making things happen need to be able to contact one another. Your committee, or core organising group, generally need to have one another's contact details so that you can all work together well. This is different from the contact details of your wider membership, mailing list or other external contacts.

Even though you all need to be in touch, it is still important to work together to protect everyone's privacy and ensure people's details are not used in ways they wouldn't reasonably expect. It is useful to make a clear agreement among your committee about how you will look after one another's contact details. This could include:

- That you will not pass them onto other people without specific consent
- That you will not use them for anything other than group business without specific consent
- That if someone leaves the committee everyone will delete their details, and vice versa, unless specific consent is given to keep them
- That you will not put other people's contact details on group publicity without specific consent.

If your committee members do not wish to share their personal contact details with each other, you could consider setting up another way for everyone to communicate. One way of doing this is to allocate each committee member with an official email address (e.g. friendsofxx-secretary@mail.com). One person should still hold everyone's personal contact details securely though, because your committee are legally responsible for your organisation so need to be contactable.

You should take care not to accidentally share personal data, including with other members of the Group. For example, if you send an email to everyone on your mailing list, do not simply type all the email addresses into the "To" field. By doing this you are actually sharing all the email addresses with everyone on the list. Use the "Bcc" field instead. This hides everyone's email addresses.

6.6 Removing Personal Data

Once you have finished using personal data for the purpose it was collected for, it should be deleted. It should not be kept indefinitely just in case you want to use it again but don't know what for. When you delete data, make sure it cannot be accessed by someone else.

You should also delete people's data when they ask you to, unless you need to keep it because of a specific legal obligation. If you send out emails to a list of contacts, you must put information at the end of *every email* explaining how to unsubscribe from the list. If you use an email newsletter provider this will happen automatically. If you send ordinary emails to a list of people, create an email signature which tells people who they should contact to be removed from the list.

6.7 People's Right to their Own Data

Individuals have a right to be given a copy of their data, and information about how it is being used. This must be provided within one month of a request. They also have a right to have their information amended or deleted within one month of a request (unless you need to keep it for legal reasons). To help you do this, make sure you know where data is being stored, and by who.

6.8 Failure to Protect Someone's Data

There are lots of ways that you might have a "data breach". These include, for example:

- Theft of a laptop or phone with contact details stored in it
- Accidentally sending an email with everyone's email addresses visible
- Sending personal information to the wrong recipient by mistake
- Losing a paper sign-up sheet on which people have written their names and addresses.

The most important thing is to recognise if something has gone wrong, so that you can take steps to reduce the impact it will have, and to avoid it happening again in future. Try to keep data protection in mind, so that you notice if there has been a possible data breach.

If you have a data breach, the first thing to do is try to get the data back. For example, if you have accidentally emailed someone's details to the wrong person, contact that person and ask them to delete the information.

The next step depends on whether the data breach is likely to have a significant impact on someone's life. If it is not likely to have an impact, you should still record that it has happened and take steps to avoid it happening again.

6.9 Data Protection Policy and Procedures

It is important that everyone involved in your group knows how to help protect people's privacy. To help with this, it can be useful to write a Data Protection Policy outlining your commitments to data protection. It is also useful to write some specific procedures which provide details of how you will ensure your policy is upheld.

Your policy and procedures should reflect the way you actually do things, so it is better not to just use an "off-the-shelf" version. To create your policy, use this section of the toolkit and make decisions about how and why your group collects, stores, uses and deletes data. A sample Data Protection Policy is provided in Appendix F.