Sponsor Refugees Guide to Data Management

Contents

What is personal data and how to we use it?

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.

You should only collect, store or use personal data if your group needs to do so for a clear, specific purpose.

CASE STUDY

Merry Street Community Sponsorship Group are organising a fundraising Iftar. To do this, they need to ask attendees for contact details, dietary requirements, and their address for gift aid donations. However, they do not need other information about people, such as their marital status, gender or age.

Writing a Privacy Notice

If you are collecting and using data on the basis of explicit consent, you should provide a privacy notice when you request the consent. 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 (*explicit consent is a valid basis*);
- 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.

You can download a Privacy Notice template from the ICO here.

Some general guidelines

- 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.

Storing data securely

Personal data must be stored securely. If your group keeps personal data in computers, your computers 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, Slack, 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.

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 on 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.

CASE STUDY

Your group's secretary keeps an up-to-date copy of all your members' contact details in their computer. Another committee member is organising an event, and needs to contact all the members to tell them about it. The secretary sends them the list by email. The committee member downloads the list into their own personal computer. (The computer should be password protected and have up-to-date anti-spyware software.) Once the committee member has done the task, they should delete the copy from their computer and emails, so that the group does not lose track of who is storing what information.

Other measures to take:

- compile and label files carefully
- keep files containing sensitive or confidential data secure and allow access on a 'need to know' basis
- keep a log so you can see who has accessed the confidential files, when, and the titles of the files they have used
- Electronic files should be password protected and stored on computers with protection against hackers and viruses.

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.

Community groups 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. Of course, if you have the group members explicit consent, you can make email addresses visible.

Deleting 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.

If someone is no longer volunteering with your group, you should delete their data. You must also inform Citizens UK, so that we too can delete their data.

It is also important that former volunteers no longer have access to confidential data, so they should be removed from forums such as Whatsapp, Google Drive and Slack, and asked to delete any data they hold.

CASE STUDY

A group member organises a day trip for the children of the family and group members. They collect information about the children's health conditions and allergies, so that they can take care of them on the trip. Once the trip is over they no longer need this information so there is no need to keep hold of it. Data that was held electronically is permanently deleted from the computer. Paperwork with health information on it is shredded.

Destroy paper documents permanently and securely
Shredding is a common way to destroy paper documents and is usually quick, easy and cost-effective. Many retailers sell shredders for use within your office or premises, enabling you to shred and dispose of the documents yourself. If possible, consider recycling your shredded documents, as long as you can do this without leaving the data easily available to others during that time.

Alternatively, you could use a shredding service. Companies will come to your business, collect the documents and safely shred them for you. If you decide to take this route, make sure you're satisfied they're a reputable company that will destroy the documents securely.

Delete digital information and any back-ups
When removing or deleting data from computers and electronic devices, you need to be aware that electronic systems can have back-ups or background storage. This may mean that information is still held for a certain period of time, even after you think you've deleted it.

When you delete data electronically with the intention of destroying it, you need to make sure it's no longer usable by you or anyone else. You shouldn't be able to still access or use the data after you've deleted it, such as through your recycle bin. Often, digital systems will hold on to data in your bin until it's automatically replaced or overwritten.

So, once you have deleted, go to your computer's recycle bin, and email's "delete" folder and delete it here also.

Safeguarding Records

We have guidance for recording and storing safeguarding information in our **Guide for Designated Safeguarding Leads**, which can be downloaded here.

If you have any questions or concerns, please contact us at communitysponsorship@citizensuk.org