GDPR/Data protection guidance for TRAs

What is data?

Personal data is any information that can identify a person. The kind of data that you might collect and handle as a TRA could be people's names, addresses, email addresses and phone numbers. You might also take photos of people at community events or make recordings of a Zoom meeting. This is all personal data or information.

Why do TRAs need to be aware of data protection?

When you collect information about members of your group or from your wider community, you are responsible for how this data is stored and how it is used. If you are collecting any personal data from people, or planning to, you should get to know the basics of data protection before you start.

Some basic tips for using data safely within your group

- Only collect the information or data *that you need to use* – don't be tempted to collect more 'just in case' or because it's interesting.
- Tell people what you are collecting their information for and specifically how you will use it. This is called a 'privacy notice' and you can read more about these below.
- If you are going to share the information with anyone else, you need to ask people first.
- Make sure that you store people's information in a safe place. If it's in a physical file, make sure it's kept in a locked drawer, or that the room where it's kept is not open to the public. If it's on a computer. Password protect both the document and your computer to make sure that no-one else can open the file.
- If you have people's contact details, check with them – maybe once a year – that they are correct and that they are happy for you to continue to use them.
- When you don't need the information anymore, dispose of it safely. For example, if it is on a sheet of paper make sure this is shredded. If it's on a computer, empty your computer's recycling bin after you've deleted the file.
- If someone asks you to delete or shred their information you must do so. You must also provide them with copies of any of the information you hold about them if they ask for it.

Collecting contact details from members or your community

If you are collecting information from people at a meeting, on a sign-in sheet for example, make sure that you don't use a communal sign-in sheet that everyone can see. Use individual contact forms, or an online contact form, for people to complete individually and give you.

Consent / draft privacy notices

A privacy notice is a statement that explains to people why you are collecting their information and what you're going to do with it. Your notice should explain:

- what their information or data will be used for
- how long you will keep their data
- whether you're going to share it with anyone (this could include Hyde staff as not all residents have given us their email address for example)
- where it's going to be stored (e.g. in a Google Drive or DropBox)
- how they can request to have their data removed

Here is an example privacy notice you could use:

XXXXXX TRA needs your contact details in order to keep you updated about our activities and to send you information about local events. Please tick the boxes below to give consent for us to use your details.

- I consent for XXXX TRA to send me details of their activities and meetings
- I consent for XXXX TRA to send me information about local events
- I am happy for XXXX TRA to add my phone number to their WhatsApp group
- I am happy for XXXX TRA to add my email address to their email group
- I am happy for XXXX TRA to share my contact details with Hyde staff

WhatsApp or other group texting apps

WhatsApp, Telegram and Signal groups are a great way of getting everyone into a single group so they can chat together and share information. However, not everyone realises that once they're added into a group, everyone else has access to their name and phone number.

Here's some things to think about with WhatsApp:

- Make sure that you check with people before you add them to a WhatsApp group. This includes letting them know what the group is for and who else is in it.
- Rather than adding people into a group, share a link to the group so they can choose whether to join or not
- Make sure that everyone is aware that other group members can see their phone numbers.
- If it is a large group, warn your members about sharing too much personal information, photos etc.

Email groups

Email is another brilliant tool for communicating with lots of people quickly and easily. It also has some risks if it's not used properly. Here are some tips for email:

- Make sure you check with people before adding their email address into an open group.
- If in doubt, use the 'BCC' tool. This stands for 'blind carbon copy' and means that other people in the group can see your email, but not everyone else's email address. They'll only see that it's come from you.
- Be careful of email chains or forwarding emails on – these can contain information further down that shouldn't be shared e.g. private conversations or people's email addresses.

Photography

Images of people are also their data, so we need to be careful to get consent when we take or share photos, especially if the photos include children.

Make sure you have a consent form signed by everyone that you want to take a picture of. The consent form should explain where the photo might be used or published. If someone is under 18 years old, ask their parent or guardian to sign the form. We have an example photography consent form that you can use for community events.

Zoom or other video meetings

Recordings or screenshots of online meetings are also people's data. If you are holding a meeting or event online and you want to take a recording, make sure that you ask people beforehand. Give people time to turn their cameras off, or to change their names on screen should they want to. Once you start the recording, confirm that the recording has started, so it's clear that everyone has agreed.

If you are holding a meeting and one of your participants has other people in their background, ask them to check that the other people in the room are ok with being visible. If children are visible, make sure that the parent or guardian is happy for them to be on screen.

If you would like more information about data protection, this website has a lot more detailed guidance:

www.resourcecentre.org.uk/information/data-protection-for-community-groups/