General Data Protection Regulation (GDPR)

- New data protection regulations have come into place since 25th May 2018
- The new regulations replace the current EU DP Directive, EU member states' own Data Protection regulations, and UK Data Protection Act 1998.
- Far more stringent & harsher penalties than existing data protection regulations
- Applies to all organisations/groups that process the personal data of individuals

What does this mean for your groups?

Basically, groups need to carefully consider how they handle personal data:

- How they collect it?
- How they store it?
- How they use it?
- How long they keep it?
- Who is responsible?

Importantly the group must understand responsibility lies with the entire group. The group is the Data Controller!

Think about the data you may store, and have contact with.

Examples:

- Record a register of attendance
- Circulation lists (email addresses) for newsletters, surveys, information
- Information about tickets for events
- Fundraising/raffles/supporters
- Volunteer information
- Other...

Delivered by smart communities part of the CCS group
On behalf of Somerset Association of Local Councils
Funded by Somerset County Council
Viney Court, Taunton, TA1 3FB
Smart Communities Limited (SCL) is a Company Limited by Guarantee, No. 11480430 and VAT Registered No. 311926619.

What is personal data?

Personal data relates to an individual's identity, such as:

- Name
- Contact details: address, phones; email; social media
- Gender, age, ethnicity (e.g., Individual DOB if collected)
- Family details
- Employee information, e.g., N.I. number
- Financial information
- Images: photos, film footage, CCTV

Map the information
Audit what data you have:

- What Personal Data does the group hold?
- Where is it held, e.g. paper files, diaries, computers, tablets, phones, memory sticks, CDs, CCTV, archives, photographs, websites, and social media?
- Who has access to it or who is it shared with?

ACTION
- Record the results
- Is the data secure? Make changes to keep it safe.

Protect your data
- You must ensure you store all personal data safely
- Any sensitive data must be protected
- Password protect your external hard drives, password protect your computer, and lock paper data away.

Reasons for collecting Personal Data

Only store the necessary data

- 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 about whether data belongs to your group or you personally. Just because you have access to contact details held by the group, doesn't mean they are your contacts.
- If you keep these principles in mind, you are likely to be respecting people's privacy and meeting the fundamental requirements of the GDPR.

Lawful (Clear purpose for processing)

Data must be handled fairly and lawfully, i.e. how it is obtained & used

- To serve your group's "legitimate interests ", or
- Because you have explicit consent from the person whose data it is, or
- To fulfill 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.

Any time you collect, store or use people's data, you should be clear about which of these reasons you have for doing so.

Can it be shared?

- Only to facilitate the group's requirements to function
- Specific consent has been given
- Already in the public domain
- Exemptions – e.g. child protection, fraud, criminal acts, breach of trust....

Legitimate interests

- Your group can use personal data if it is in your group's legitimate interests. This means that you can use data in ways that are necessary to run your group.

- You should only use the minimum amount of data that you need, and you should give people the option of having their data removed from your records.

For example, a list of who is part of the Steering group, their name, and how to contact them via an email address or telephone number.

Consent

- Your group can use personal data if you have explicit recorded consent. Consent is only valid for the particular purpose it was gained for.
- People must be well-informed to give consent. You must explain why you need the data and what you will use it for, and that the person can ask for it to be deleted in the future.
- To use consent as a basis for using data, you must keep a clear record of who has given you consent and for what. Consent must be positively given. You cannot assume consent just because somebody has not said anything. When using tick boxes, people must be required to tick a box to give consent. Pre-ticked boxes do not count.
- You can get verbal consent, but you should still explain specifically what the data will be used for and that they can ask for it to be deleted in the future. You still need to keep a written record so that you know who has given you consent and for what.

Legal obligation

- Another common legal reason a community group might have for using personal data is to check the criminal records of their volunteers. This is a legal requirement for some types of work with children and vulnerable adults. To check criminal records, groups must share personal data with the Disclosure and Barring Service. However, they should not keep hold of data relating to people's criminal convictions. For example, once a group has established whether someone is a suitable volunteer, they no longer need to hold the information and should delete it securely.

GDPR allows Groups to lawfully hold Personal Data that is specifically held for the 'purposes of running your group'

However, if it is held or used for other purposes (incompatible with the group's purpose) - obtain consent to use it!

ACTION

- Positive affirmation required, e.g., tick box, signed consent form
- (A 'Yes' to receiving information as a record of the consent)

Privacy Notice: what is in one?

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 that 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 do 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 based on explicit consent, you should provide a privacy notice when you request consent.

Privacy Notice: Legitimate Interest Example

" *XXXXX Group has your contact details because you have attended one of the sessions in the last 12 months. We only use these details to send you information about our future s*essions. We do this because it is in the legitimate interest of our group to publicise our sessions to regular attendees. Your details are stored securely by XXXXX group and will be deleted if you do not attend a session for 12 months. You can ask us to amend or delete your details at any time by contacting the Secretary on Tel:....."

Privacy Notice Example: consent

XXXXX Community Group needs your name and email address to send you information about group activities. Please tick the boxes below to give consent for us to use your details.

☐ I consent for XXXXX Community Group to send me details of their events and meetings.
☐ I consent for XXXXX Community Group to send me information about their campaigns.
☐ I consent for XXXXX Community Group to send me fundraising appeals.

Your details will be stored securely online in our Google Drive folder and will be removed within one month if you end your membership of XXXXX Community Group. You can withdraw your consent for us to use your information, or ask us to amend or delete your details, by emailing secretary@XXXXX.org.uk.

Privacy Notice Sample:

We look after your information carefully. We are collecting your information so that we can let you know about how to attend our events and activities [you can give some examples here], either because you have expressed interest, or you have already come along to something. We will hold your information for a year after you stop coming to our events and activities. [It's up to you to decide how long you need to keep the information, you should be able to explain why] If you want to update your information at any time, please contact...
We do not share your information with anyone unless required to do so by law, or with your explicit consent. You have rights over your data under UK and EU law.

FYI: The Information Commissioner's Office has some great resources to help you understand these rights and how you can apply them.
Visit: https://ico.org.uk/

Sharing personal data with others

- 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 sharing all the email addresses with everyone on the list. Use the "Bcc" field instead. This hides everyone's email addresses.

- This is especially important if your group members all share a particular personal characteristic (e.g. a group for people who are LGBT, or a group for survivors of domestic abuse). Accidentally sharing the names or contact details of your group members could mean revealing that they have a particular personal characteristic, which they may not wish to be public knowledge, and which could affect their lives in significant ways.

Photos

- If you take a photo at an event, you hold you must have permission from those people in the photo to use it.
- Your face is your property!
- If there are children in the photo under the age of 13 then you must have guardian consent.
- You can ask them to sign a release form.
- It is best, if possible, to stand back and take a photo at a distance to remove the need for release forms.
- Or find Licence Free images online here: https://pixabay.com/ or https://www.canva.com/

Further information and resources

- Consult the ICO website – www.ico.org.uk
- ICO Helpline for small organisations: 0303 123 1113 (select option 4 to be diverted to staff who can offer support. A live chat is also available

Free templates and advice for Community groups are also available from the Resource Centre
www.resourcecentre.org.uk

Here is a direct link to the Data Protection for Community Groups:
https://www.resourcecentre.org.uk/information/data-protection-for-community-groups/