FOR ORGANISATIONS

DATA PROTECTION

In these unprecedented times, we understand that local communities want to do their bit to support each other. This should be commended, as without the support of community volunteers, those in the most need, run the risk of being isolated. However, we are also assuming that volunteers will need handle some personal information relating to the individuals they are supporting. As a result, you and your group need to be aware of important data protection principles.

What do you need to consider?

- Consider the task you are carrying out and just obtain the information you need.

- If you need to share the information you've obtained with someone else, make sure they are the only recipients, and that they know not to share it on further.

- Once the information is no longer required, destroy it securely (preferably by shredding).

Shopping for individuals

- You may be in possession of sensitive, personal information i.e. medical conditions - respect the privacy of the individuals who are trusting you to support them. Make sure this information is well protected, not shared with anyone and destroyed securely afterwards.

- If you are trusted with an individual's bank details or payment cards, treat them as if they were your own - keep them safe and do not use them for anything other than the purpose that has been specified.

Voluntary Action
North Somerset

FOR ORGANISATIONS

DATA PROTECTION

Maintaining contact lists

- If you are holding a database of the individuals you are supporting, ensure the minimum amount of information is held for you to be able to delver the service.

- Volunteers should be reminded of the importance of protecting the privacy of individuals information at all times.

- If volunteers require to be DBS checked to deliver a service, you only need to have sight of their certificate, you do not need to retain a copy.

Using social media and online video platforms

- When using Skype or producing YouTube videos be mindful of what else can be seen through the camera feed. Remember videos can be paused and images zoomed in on.

- Open social media groups allow anyone to view the posts and if personal information is posted, this information is being made public.

- Consider using a 'closed group' that is closely managed by a team of administrators.

- Pay attention to the type of information shared on your social media platforms and ask the question if it is 'sensitive' or relates to 'vulnerable' individuals - if you would feel uncomfortable or concerned if information about yourself was being posted, then it is likely that it should not be posted.

Voluntary Action
North Somerset

FOR ORGANISATIONS

DATA PROTECTION

- As custodians of social media platforms, with a closed group make sure subscribers agree to terms and conditions of content.

- Make sure 3rd party posts are managed appropriately and they fall outside of the terms and conditions of the objectives of the group, delete them.

Information scams

There's no easy way of preventing scammers, especially when they're targeting individuals who aren't the most IT-literate. Just reiterate the messages all the time that no official organisation:

- will ever ask them to divulge any personal or security details.
- will ever phone them out of the blue and ask them to do something.
- will ever email them directly with web links or attachments containing 'official advice'.

When the crisis is over

You should keep a record of any decisions you make that involve the use of personal information. Ideally, you should do this first – even before you start collecting information (that might not be possible during the pandemic). Make sure you keep notes of what you've done and why and make more detailed records as soon as possible.

Where can I go for more help?

The Information Commissioner's Office for general advice: www.ico.org.uk and for Data Protection & Coronavirus info: https://ico.org.uk/for-organisations/data-protection-and-coronavirus/

Voluntary Action
North Somerset