Blog: Community groups and COVID-19: what you need to know about data protection

A blog by Ian Hulme, Director for Regulatory Assurance at the ICO.

As COVID-19 continues to sweep across the UK, more and more people are driven to help the most vulnerable in our communities. Church groups, neighbourhood and residents associations are being set up to support the work of existing community groups, services and charities.

Often, these groups need to handle sensitive personal information and share it with others. And that means taking account of data protection law.

If you've just formed a community group, this may be the first time you've had to think about data protection. Put simply, the law is a set of sensible standards that will help you handle people's information responsibly. That means taking proper care of things like people's names and addresses as well as more sensitive details about their health or religion.

Crucially, data protection rules will not stop you from helping those in need.

This blog is intended to clarify some of the basics of data protection, and to give established community groups, services and charities clarity on how to apply the law in this extraordinary time.

We've also published Q and As for organisations that might help you. If you still need help, we're here to answer your questions. Ring us on 0303 123 1113.

Keep it clear

You should be clear, open and honest with people about what you are doing with their personal information.

Tell them why you need it, what you'll do with it and who you're going to share it with.

It's best to have this written down in a document called a privacy notice – here's a template you can use. But if that's going to delay vital support, then you can just speak to people.

Keep sharing

In an emergency, working with partners and sharing information with them can make a real difference to public safety. In fact, it could be more harmful not to share the data than to share it.

For example, you might need to tell a local council about elderly residents who are housebound due to self-isolation and who need support.

If you can, think ahead. What kind of information are you likely to share? What do you need to do to make sure that happens securely?

Data protection law does not prevent you sharing personal information where it is appropriate to do so.

Keep it lawful

If you're not sure whether you should be handling personal data, think about whether it falls into one of the following categories:

- Would the person expect me to use their information in this way (legitimate interests)?
- Have they given me their clear and unambiguous consent to use their personal information (consent)?
- Is the person's health or safety at risk if I don't use their personal data (vital interests)?

If the answer is yes to any of these questions, then you can handle and share personal data.

You should also take particular care if you're handling sensitive data, referred to as 'special category data' in data protection law. This is private information like your health records, sexuality, race, ethnicity and religion. If you are going to use this kind of information, you should ask further questions:

- Do I need this information to protect a person at risk (safeguarding individuals)?
- Have they given me their explicit consent to use their private information (consent)?
- Would this information save someone's life (vital interests)?

If the answers is yes to any of these questions, then you can also handle and share this type of information. Make sure you are doing only what is necessary and appropriate for the task at hand.

Keep it secure

You must look after the personal data you collect. That means keeping it secure on a device – which can be your own - or in a locked cabinet, for example.

Security measures needn't be so onerous that they prevent you carrying out your work.

Think about the impact on a vulnerable person if the information they entrusted you with becomes lost or stolen. Then apply measures to reasonably reduce the risk of that happening.

We've created some simple security tips for community groups.

Keep it to a minimum

Only use and keep what you need to provide help to vulnerable people during the COVID-19 crisis. When the emergency is over, make sure you and your volunteers securely delete or destroy any personal information that you no longer need.

Keep a record of what you've done

Finally, 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. But we understand that might not be possible during the pandemic. So just make sure you keep notes of what you've done and why and then make more detailed records as soon as possible.

Ian Hulme is Director of Regulatory Assurance at the ICO.