What does GDPR and data protection policy mean for your organisation?

Data protection legislation – General Data Protection Regulation (GDPR) – applies to any organisation with data on staff, volunteers, donors, or service users. GDPR also applies to non electronic use or storage of date.

Key actions required by GDPR are set out below:

- As a minimum, you need to understand what personal data is being processed where, by whom, and for what purpose.
- Collecting consent on an opt-out basis is no longer valid.
- You must document the legal basis on which you process data from the six possible options here. For charities, this is likely to be: because you have asked people if you can; because it is part of your contract to deliver a service; or because you have a 'legitimate interest'.
- Look at the information you give to people about how their data is processed. What you do with data should be set out in a privacy policy or a fair processing notice.
- The most common data breaches are caused by human error. Develop or review your data protection policy and train staff in how to keep data safe. Document how you will report any data breaches.
- People can request the data you hold about them, and you will have a month to comply with their request. Develop procedures for enabling people to access the data you hold about them and test your systems on how to retrieve data.
- Document your processes. The responsible authorities understand that data breaches, such as cyber hacking, can happen to big and small organisations as a consequence of the digital age we live in. It is the process you use to safeguard personal data that is of importance.

Source: www.impactsupport.org