Voluntary Action South Lanarkshire Briefing:

General Data Protection Regulation (GDPR)

The **General Data Protection Regulation (GDPR)** is a new EU law that will come into effect on **25 May 2018** to replace the current Data Protection Act.

It is the biggest overhaul of data protection legislation for over 25 years, and will introduce new requirements for organisations on how they process personal data, and has greater emphasis on organisations accountability of data.

It has also been made clear that after Brexit, all businesses and charities will still need to comply, which means that the UK will likely adopt all or most of GDPR as legislation.

Data protection requirements will apply for campaigning, marketing, managing volunteers and recording information about service users – anything that involves processing an individual's personal data.

Charities will need to adopt a whole organisation approach, with a strategy agreed at Board level. Volunteers are no different to employees; they must be trained and equipped to protect data. Don't leave it until the last minute, as you may find compliance difficult if you leave your preparations to nearer the deadline.

Key Changes:

- GDPR requires organisations to maintain records of what data you hold, where it came from and who you share it with.
- Under GDPR simply saying 'Click here to read our privacy policy' is no longer enough. You need to explain clearly why you are collecting personal data, and how you intend to use it. If you intend to make any data available to third-party providers you need to get explicit consent for that.
- For consent to be valid, it will need to be freely given, specific, informed and a clear affirmation action, such as actively ticking a box on a form electronically or physically.
- New emphasis on individual's rights to access their own personal data. This means people can make access requests at any time to check the data you hold and what you do with it. You need to plan how you will handle any

requests within the new timescales (1 month rather than current 40 days) to avoid making it too onerous and time-consuming.

- GDPR also brings in rights for people to request the removal of personal data, this might be because they no longer want you to have it or if it is no longer used for the purpose it was collected. Data has to be kept up-to-date and accurate and organisations need to ensure they are not keeping data for longer than necessary. Processes to cover this could include 'Find out what information we have" or "Remove all information about me" sections in an organisation's privacy policy to give people clear information.
- The amount the Information Commissioner's Office (ICO) can fine organisations for breaches of data protection has been increased, and there is a new duty on organisations to report certain types of data breach if they occur.
- When you collect personal data you will need to tell people your identity, how you intend to use their information, your lawful basis for processing the data, your data retention periods and that they have a right to complain to the Information Commissioner's Office if they think there is a problem with the way you are handling their data. This must be given in concise, easy to understand and clear language.
- Personal data in the public domain is not exempt, and certain sensitive data: racial or ethnic origin; political opinions; religious beliefs; membership of a trade union; physical or mental health or condition; sexual life; information about criminal convictions and any criminal proceedings has stricter requirements.

Other Useful Information:

- To help organisations, the Information Commissioner's Office (ICO) have produced a 12 Steps guide which organisations should use as a first step to ensure they will comply before the deadline.
- Fundraising and Data Protection by Tim Turner will be very useful for charities and groups who fundraise