Data Protection

This information sheet provides a brief overview of the main requirements of data protection legislation and its implications for voluntary and community groups. New data protection standards were introduced by the European Union under the General Data Protection Regulation (GDPR) and this was enshrined in UK law by the Data Protection Act 2018.

What is covered by data protection legislation and does it apply to your organisation?

Data Protection is all about handling personal information responsibly and taking steps to ensure it is secure and not misused. Your organisation is almost certainly covered by the legislation, even if all you do is keep a list of members' contact details.

The data covered is any personal information in any format. This could include paper files, such as membership forms, attendance sheets, diaries and minutes of meetings, and also personal details that are stored electronically, such as on a computer. It also covers other information, including photos, CCTV footage or other images, the IP addresses of people visiting your website and e-mails. The legislation covers the processing of data from collection to storage, usage, how it is organising, updating and amending, sharing and finally destroying the data.

There are **six primary Guiding Principles** which should be adhered to and makes your group accountable when processing personal data to ensure fairness:

1. **Lawfulness, fairness and transparency**: Data should be processed lawfully, fairly and in a transparent manner.

2. **Purpose limitation**: Data should only be collected for specific, explicit and legitimate purposes.

3. **Data minimisation**: Data should be adequate, relevant and limited to what is necessary.

4. **Accuracy**: Data should be accurate and, where necessary, kept up to date.

5. **Storage limitation**: Data should be kept only for as long as is necessary.

6. **Integrity and confidentiality**: Data should be processed in such a way as to ensure the integrity of the data and the confidentiality of the data subjects.

Glossary of Key Terms

Data Controller: any person or organisation that decides what personal data to collect and how to process it.

Data Subject: any living person about whom you collect, hold or use personal information.

Data Processing: from the moment you take someone's details to the moment you shred or delete their file, you are processing data about them.

Data Processor: any person or organisation that processes data on behalf of another but not employees of the Data Controller.

Personal Data: any information relating to a living person who can be directly or indirectly identified because of the information.

Special Categories of Personal Data

Previously called sensitive data, these categories include information relating to:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data used to uniquely identify natural persons
- health data
- data concerning an individual's sex life
- sexual orientation

What are the practical implications?

The data isn't yours! The data that you collect about your members or beneficiaries isn't yours: it belongs to the individual and they can instruct you to stop processing their data, insist that you correct any errors and generally decide what you may or may not do with their data. An individual has **eight rights** to their data: the **right** to be informed, **right** of access, **right** to rectification, **right** to erasure/to be forgotten, **right** to restrict processing, **right** to data portability, **right** to object and **rights** in relation to automated decision making and profiling.

Better communication: you need to tell people why you are collecting their data and what you intend to do with it. You should tell them this at the point of collecting the data by giving them a Privacy Notice or access to a notice such as on your website.

You will probably need consent: you may well need signed consent before you process personal data, but there are five other legitimate reasons why you may process data, depending on the circumstances,

including to enter into a contract, to meet a legal obligation, to protect the vital interests of a subject, to perform a task that is in the public interest and to pursue a legitimate interest.

Responding to a subject access request: if someone asks for all the information you hold on them then you must provide it within a month and at no charge. Only in exceptional circumstances can you ask for more time and, even then, you are limited to two months.

Dealing with a data processor: if you ask another person or organisation to process data on your behalf, e.g. to evaluate a project or provide statistics, then you need to enter into a formal contract that specifies the obligations of both parties.

Data retention: your privacy notice and data protection policy should specify how long you intend to retain data.

Privacy by design and default: when starting a new project data protection should be one of the first topics you consider. Think about the security measures you must put in place to protect the data.

Children: young people under 13 years of age must be given special consideration particularly in relation to obtaining consent.

Registering with the Information Commissioners' Office: You are not required to register with the ICO and pay a fee if you are only processing personal data for staff administration, accounts and records, not-for-profit reasons, personal or family affairs, and advertising, marketing and public relations purposes. You are also exempt from registering if you only keep paper records and do not use an automated system such as a computer to process personal information but this does not mean you are exempt from complying with GDPR and other data protection laws.

However, even if you fall into one of these categories but your organisation uses CCTV for crime prevention purposes, you will need to register and pay the fee. You can use the ICO self-assessment form to determine if you are exempt or not. If you are still unsure whether or not to register, do call their helpline 0303 123 1113.

Data breaches: a breach of security leading to the destruction, loss, alteration, unauthorised or accidental disclosure of, and access to, personal data may need to be reported to the ICO. If an incident does need reporting it must be done within 72 hours (3 days) of becoming aware that is reportable. If you are unsure whether to report the breach you can check the ICO website for details, ring their helpline 0303 123 1113, or contact them via live chat; they are very helpful and supportive.

Additional Support

Community First Yorkshire can help you with any question you may have about running an organisation, being a trustee, funding, fundraising or volunteering. We can support you on a one to one or group training basis. Simply fill in an **enquiry form** and we'll get back to you.

You can sign up for our news bulletins **here**:

- Our monthly Funding Bulletin lists updated funding opportunities.
- Our weekly newsletter has information about the volunteer and charity sector, including training courses about funding.

Updated: 20 September 2021