Data Protection
Guidance notes for Support Groups

The Data Protection Act 1998 controls how your personal information is used by organisations, businesses, or the government. Everyone who is responsible for using data has to follow strict guidelines called ‘data protection principles’ – failure to do so would be breaking the law.

In addition to the eight principles, the Data Protection Act also provides individuals with some important rights;

- the right to access the information that is held about them
- compensation for mishandled information
- prevention of the processing of information

The Information Commissioner’s Office (ICO) polices Data Protection and will take legal action against groups and organisations that are not compliant.

There are eight principles to follow to ensure that the personal information is;

- **used fairly and lawfully**
  Members must give their permission for you to store and process their data. It would be good practice to ask members to complete and sign a contact form for your database. Access to this information should be limited to certain member(s) of the group with specific roles

- **used for limited, specifically stated purposes**
  Members must be told what information is being stored and how it will be used. Do not share their data with any third party (including other members) without permission.

- **used in a way that is adequate, relevant and not excessive**
  Only request personal data that is relevant – do not collect information not relevant just because it might be useful for the future

- **accurate and up-to-date**
  Ensure data collected is accurate and update information on a regular basis. i.e. contact forms can be updated on an annual basis

- **kept for no longer than is absolutely necessary**
  i.e. if some members have stopped attending group meetings and have no other interaction with the group, then they should be given the opportunity to be removed from the database – there should be an ‘opt out/opt-in’ policy. If a member asks for their information to be removed from the database, you must ensure that it is permanently deleted from your computer records and that any hard copies are shredded

- **handled according to people’s data protection rights**
  Members have a right to know what information you hold about them and
If you do not handle data correctly and cause harm to an individual, they will have a right to compensation. You must ensure that data is accurate, adequate and kept confidential.

- **kept safe and secure (i.e. password protected, locked storage)**
  Use passwords to access computer equipment and databases, and info should only be accessed by authorised people. Hard copy information should be kept safe and secure in locked drawers/cupboards. Use the Bcc facility when sending bulk emails.

- **not transferred outside the UK without adequate protection or consent**
  Transferring data outside of the UK must still be protected and you must obtain members consent to do so. Any personal data that is shared on your website would also require consent.

The top five data protection tips from the Information Commissioners Office (ICO) for small and medium organisations are;

- Tell people what you are doing with their data
- Make sure that the people responsible for handling the data in your group are adequately trained and aware of the data protection principles
- Use strong passwords – strong passwords usually contact a mixture of upper and lower case letters, a number and a symbol
- Encrypt all portable devices (i.e. memory sticks, laptops) – you can use an encryption tool such as BitLocker but this may not always be possible for very small groups which is why you should at least ensure that passwords and locked storage is utilised
- Only keep people’s information for as long as necessary (ensure that data stored is regularly updated/deleted)

Please also bear in mind that there is stronger legal protection for more sensitive information, such as;

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

For more information about the Data Protection Principles please visit;

Gov.UK website

Information Commissioner’s Office
[https://ico.org.uk/for-organisations/](https://ico.org.uk/for-organisations/)

Please note that small not-for-profit groups and organisations do not have to register with the ICO but must still adhere to the Data Protection principles.