

ADVICE SHEET 5

DATA PROTECTION

Aims of the Data Protection Act

The Data Protection Act obliges everybody to process personal data in accordance with the law. Its aim is to balance the rights of individuals with regard to how their information is processed with the legitimate need of organisations to use information.

U3As as not-for-profit organisations are exempt from registration provided that:-

1. The processing of personal data is only for the following purposes
 - Establishing or maintaining membership
 - Providing or administering activities for individuals who are members.
2. The persons about whom the data is held are current or prospective members.
3. The type of data held is only that necessary to undertake the purposes above i.e. names, addresses, identifiers.

Obligations under the Act

Even though U3As do not need to register, they must still comply with the other requirements of the Act and remain subject to penalties if offences occur. Most importantly the processing should be in compliance with the Eight Data Protection Principles. These determine how personal data should be processed in order to comply with the Act and give rights to individuals regarding this processing.

The Eight Data Protection Principles

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any matter incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Things to consider

1. Do the people whose information is held know what it is going to be used for?
The best way is to put a statement on your membership form that the supplied data will be held and maintained on a computer for the purposes of correspondence/contact. If you haven't done this in the past, you would be advised to mention it in your newsletter.
2. Is it accurate and up to date?
You must ensure that you make changes quickly to all copies.
3. Is it deleted and destroyed if the person leaves?
4. Is it held on a strict need to know basis?
Ensure that you limit the number of committee members holding the full database to the absolute minimum. If there are other members of the committee who need contact details, just supply them with email addresses and telephone numbers. If group leaders/convenors require contact information, the best way is for them to request it from their group members.
5. Is it held securely?
Password protect the database and avoid issuing hard copies unless you have no choice.