An introduction to.....

sloughcvs
www.sloughcvs.org.uk

Data Protection

Any organisation that collects personal data about individuals is known as a 'data controller' and must comply with the requirements of the Data Protection Act 1998. The aim of this factsheet is to provide an introduction to the Act along with some basic information about complying with its data protection, storage and disposal requirements.

The Data Protection Act 1998

The Data Protection Act sets out eight principles that anyone processing data should follow. These state that data must be:

- processed fairly and lawfully;
- processed only for specified particular purposes;
- adequate, relevant and not excessive for the purposes for which it is kept;
- accurate and up-to-date;
- not kept for longer than is necessary;
- processed in accordance with the subject's rights;
- kept with appropriate security measures, e.g. through the use of lockable filing cabinets, password protected computerised systems, the implementation of a confidentiality policy etc.
- not transferred to countries outside the EEC without adequate protection or consent from the individual/s concerned.

The Act, therefore, provides a framework to ensure that organisations handle personal information properly. It also protects individual's rights by ensuring that they have access to the personal information that is held about them.

If your organisation handles personal information, it is therefore good practice to have a policy that covers data protection. This is particularly important for organisations that carry out Disclosure Barring Service checks on individual's they employ or work with. In addition, you must register with the **Information Commissioner's Office (ICO)**. (There are some exceptions to this, for example, where personal information is only being used for staff administration purposes.) The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act, including the power to issue information and enforcement notices, conduct audits and prosecute offenders.

Data Protection Policy

The areas a policy should cover are:

- What information will be collected and why;
- How long the information will be kept for;
- How the information will be stored;
- How an individual can access the information held about them.

For most organisations, the main things to bear in mind when writing and implementing a data protection policy are to ensure that:

- everyone that you hold information about knows that you do and has given permission for it to be stored and used;
- records are not held for longer than necessary and are stored and disposed of securely;
- records are held in such a way that individuals who wish to see what information you hold about them can do so.

The Data Protection Act also defines what is considered 'sensitive' data, which covers information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, criminal record or proceedings relating to an individual's offences. This type of information will often be collected as part of the recruitment process for staff and volunteers so it is important that your policy covers your organisation's procedures for the handling, use and retention of such data.

For example, records that are held for the purposes of recruitment should be destroyed either as soon as a decision has been taken on whether or not to employ the person or within 6 months. Equal opportunities monitoring information should ideally be collected / stored anonymously and only be used for reviewing how your organisation's policies and procedures are ensuring equality of opportunity.

Further information about data protection can be found on the Information Commissioner's Office website at **www.ico.gov.uk**

Slough Council for Voluntary Service is an infrastructure organization that provides support to the voluntary sector in Slough. However, we cannot offer legal advice – for such you should consult a legal expert.