Data protection

The Data Protection Act 1998 is the law that governs the processing of personal information held on living, identifiable individuals. You must comply with the Act if your organisation processes personal information.

The Act requires that you are open about your use of information and follow certain principles for processing that information. The Act covers information that is:

- Held on any relevant filing system (this includes paper systems about clients and files on service users)
- Stored on any form of computer or automated filing system
- Any information that is intended to be placed in either of the above systems

Much of the Act applies to the **Data Controller** – this is the person or people who are identified as being responsible for deciding how personal information will be used in any organisation.

In many cases this is not a person/people in isolation but is the organisation itself and individuals within the organisation are classed as agents of the Data Controller.

The main focus of the Data Protection Act is the eight Data Protection principles:

- Data must be processed fairly and lawfully
- Data must only be used for specific purposes
- Data must be adequate, relevant and not excessive
- Data must be accurate and kept up-to-date
- Data must not be kept for longer than necessary
- Data Subject's rights must be respected

- Organisations must take appropriate steps to maintain security – ie prevent unauthorised processing or accidental loss, damage or destruction

- Data must not transferred abroad without adequate protection

The Act does try to strike a balance between the needs of the **Data Subject** and the Data Controller. For example advice giving organisations may hold information about other organisations or individuals for the sole purpose of passing on to clients.

Examples of personal data include:

- Client or case records
- Records of staff and volunteers
- Membership records
- Newsletter mailing lists
- Fundraising or supporter databases
- Contact databases
- Lists of trainers, consultants or other resource people

The Act creates additional obligations in respect of sensitive data about individuals.

These principles and the rights given to individuals are designed to enable people to:

- Access information about them
- Check it is accurate, relevant and up-to-date – and have it changed if it is not
- Ensure they are not unfairly prejudiced or harmed by it and how it is used

How the law affects community and voluntary groups

Rights of individuals to access data

Your employees, volunteers, clients and users have the right to know almost all the personal information that is held about them, both manual and computer data **unless one of the exemptions apply.** You can withhold access by a Data Subject to information held about him/her if it also contains information about a third party and which could prejudice the rights or interests of that person if disclosed. This could be because:

- You owe a duty of confidentiality to that person
- Or you have not been able to get his/her consent to disclosing the data or she/he has not been able or willing to give consent
- And it would not be reasonable to disclose without consent

Many organisations now produce Data Protection and Privacy Statements that set out Data Subject's rights to access and to fair processing and explain any opt-outs they can exercise (eg to ask for their information not to be used for direct marketing or not to be disclosed to other organisations)

In general though you do have to provide a Data Subject who asks for it, with a copy of all information held about them except where:

- She/he is not entitled to access (see above)
- Or it is not possible or would involve 'disproportionate effort' to provide the information.

This does not mean inconvenience, there has to be a genuine reason and the Office of the Information Commissioner has issued guidance on this. Website www.ico.gov.uk

A request must be made in writing, email and fax are acceptable. A fee of up to £10 can be charged and data does not have to be disclosed until the fee has been paid. Proof of identity may be made and all valid requests should be dealt with within 40 days of receipt.

Data Protection and the Internet

When putting information on your website you should remember that information can be accessed by anyone, anywhere in the world.

The very least your organisation should be doing if you are publishing a list of contacts is to get prior agreement from those whose information is going to be published that this is acceptable.

It is especially important to consider issues of privacy if photographs of identifiable individuals are going to be used. This information is considered as an overseas transfer and should be treated as such.

Key Points for Organisations

- ❖ As far as possible, get consent for the information you hold. If you hold sensitive information then written consent is the best way to protect your organisation.

- ❖ Make sure that everyone you hold information about knows it, why, how long you intend to hold it and who you might share it with. A statement on publications such as leaflets and any forms that you require to be completed can cover this.

- Give people or organisations the option to opt out of any direct marketing and modify your systems to suit this.

- Make adequate security arrangements for both paper and computer records eg secure filing systems, password protected computers.

- Draw up a Data Protection Statement and Policy and security measures – this may be part of your Confidentiality Policy.

You can obtain further information on Data Protection from:

The Information Commissioners Office – www.ico.gov.uk

Useful publication:

Data Protection for Voluntary Organisations
Paul Ticher: £18.95 Directory of Social Change

RCVDA has a copy of this available for groups to access at our Redcar office.

Redcar & Cleveland Voluntary Development Agency
Westfield Farm
The Green
Dormanstown
Redcar TS10 5NA

Tel: 01642 440571
Email: enquiries@rcvda.org.uk