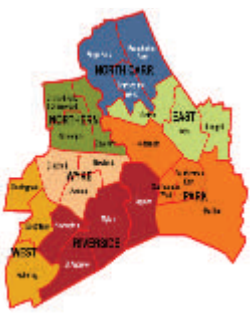
Data Protection Getting Started

Hull CVS
'community and voluntary services'



Introduction

In 1984 the first Data Protection Act came into force. It required anybody who processed **personal data** on a computer or other electronic retrieval system to Register with the Data Protection Commissioner. For the most part, voluntary and community organisations could afford to pay little attention as in those days computers were less commonly used by them.

In 1998, to comply with new regulations from the EC, a new Data Protection Act came into force. This Act is a little different, and we can no longer afford to ignore the issue partly because of the different requirements it contains, and partly because more voluntary and community organisations now use computer technology to process information about people.

Data Protection can seem very confusing and complex. Remember, it covers all kinds of things from direct marketing to client records.

What you need to know is whether or not the provisions in the Act apply to anything that your organisation or group does.

What is Data Protection?

Data Protection is all about treating **personal information** about **living individuals** in a **fair** way and making sure that it can't be **used or misused** in a way that it can cause **harm or distress**.

For example, when organisations persist in sending mail to a deceased loved one, how upsetting is that for the family? How would you feel if an organisation passed your details on to another organisation when you didn't realise they were going to do that and they didn't ask you first? And how would you feel if they *didn't* pass your details on when you expected that they would and you needed them to? What a waste of money it is sending mail to people who don't want it, and how annoying it is for them! Do you get sick and tired of junk mail? Would you expect a professional person that you've consulted to accidentally leave your file on a train? If an organisation asks you for your details, do you trust them?

These are all Data Protection issues. For some living individual out there, your organisation could be the one in question.

The Data Protection Act 1998

The Data Protection Act 1998 covers personal information about living individuals. It covers that information when it is held on a computer or other electronic retrieval system. It covers manual files if they are arranged in such a way that you could look somebody up (for example alphabetically by name). It covers other information too, including photos; CCTV footage or other images. It covers processing of that data from collecting it to storing it, using it, organising it, updating it, amending it, sharing it and finally destroying it.

Hull CVS
'community and voluntary services'

The Data Protection Act 1998 lists 8 principles by which personal data should be processed:

	The Principle	What it means
1	Personal data shall be processed fairly and lawfully	Speaks for itself
2	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes	The Act defines purposes (e.g. staff administration). If you collect data for that purpose, you can't then use if for another purpose (e.g. to try and sell them something) or for a purpose that isn't lawful.
3	Personal data shall be adequate relevant and not excessive in relation to the purpose or purposes for which they are processed	For example, do you ask people for their date of birth? Why? Do you need that information? If all you need to know is that they are over 18, just ask if they are over 18. You don't need to ask their date of birth.
4	Personal data shall be accurate and, where necessary, kept up to date	This means you need to check and periodically review information.
5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes	If you don't need to keep someone's details, don't. If you only need to keep it for a specific reason, destroy it once that reason no longer applies.
6	Personal data shall be processed in accordance with the rights of data subjects under this Act	You will need to know what their rights are if you are to respect them. For example, one right is the right to see what information you hold on them. Would your organisation know how to respond if someone asked to see the information you hold on them?
7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to, personal data	This means you have to make appropriate arrangements for security. Lockable filing cabinets; up to date anti-virus software; policies and training for your staff and volunteers for example. This is part of the information you have to supply when you send your notification to the Commissioner.
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.	This is only likely to affect those voluntary organisations working with developing countries, or it could be an issue for groups working with newcomers to this country.

What do you need to do?

There are 5 things you need to do to get started:

1. Check whether you process any **personal data** in a way that falls under the Act – i.e. whether or not you are a **Data Controller**

And if you are:

2. Check whether any of the data processing you do means that you have to **Notify** the Data Protection Commission (and be included on the register of Data Controllers)

3. Adopt a Data Protection Statement and Policy

4. Check that all the data processing you do conforms to the **8 Principles** in the Data Protection Act.

5. Make sure that people know what personal information that you have about them and how you use it.

1. Are you a Data Controller?

At the very least, your organisation will probably keep a list of its members' contact details. If you are a not-for-profit organisation, and that is all the information you collect and use ever, then you are not likely to be a **Data Controller** as defined by the Data Protection Act 1998 and probably need do nothing more – but don't take our word for it – look at the sources of information and further reading section and check to make sure.

If you collect any other information about any living individuals and keep it in any kind of filing system that would allow you to look somebody up then you probably are a **Data Controller** and you will need to make sure you are processing that information lawfully. It doesn't matter whether your organisation has premises and staff, or whether your secretary does it all from home, you do need to comply with the Data Protection Act. Having a policy and rules about confidentiality is not enough. Data Protection is not the same thing as confidentiality.

2. Do you have to notify the Data Protection Commission (i.e. Register)?

Under the 1984 Data Protection Act, you had to Register. Under the 1998 Act, you have to **Notify** the Data Commissioner if you process data for certain purposes.

There are some exemptions (we have already mentioned membership lists for not-for-profit organisations). If all the processing you do is exempt you can still Notify voluntarily.

To find out more about when you have to Notify, see further help and reading at the end of this handout. If the data processing you do is required to be notified, you must notify. It is a criminal offence not to.

3. Adopt a Data Protection Statement and Policy

A **Statement** is just that – a statement saying that your organisation complies with the Data Protection Act 1998.

Your **Policy** will depend on the size and scale of the organisation and the scope of the work you do, as well as the kinds of data you process. If all you do is keep a newsletter mailing list, your policy might not need to be very sophisticated. If you keep records on vulnerable clients; staff and volunteers; people who donate money; networking

groups; and the financial details of people who pay you money, then you will obviously need a much more robust policy.

Your policy should certainly cover a few key points:

- Who is designated as your **Data Protection Compliance Officer** who will ensure that your organisation complies with the requirements of the Data Protection Act 1998.
- The data you process including what data you collect, whose data it is, how and why you process it
- Your systems and procedures for keeping it all up to date and accurate
- Your systems and procedures for storing and handling it
- Any rules your staff/volunteers/members have to follow
- Any special rules about sharing information with other organisations
- Your system and procedures for disposing of information you no longer need or that is out of date
- How you are going to make sure all your staff and volunteers know what they can and can't do
- References to related policies, e.g. confidentiality policy; staff recruitment and selection policy; child protection policy; vulnerable adults policy; use of IT policy and so on
- How you make sure people know what you do with their details
- The date your committee or other governing body adopted your policy and when it will be revised.

4. Audit your Data Processing

Firstly, you need to list all the processing of **personal data** that you do, to check which things come under the Act. Here are a few examples:

- Databases
- Staff and/or volunteer records
- Client files
- Referral forms
- Mailing lists
- Correspondence files
- Email address books
- Website reply forms
- CCTV footage
- Booking or application forms
- Invoices

Then you need to check whether any of these have any special considerations, for instance if you keep notes on medical conditions of staff or clients, this counts as **Sensitive Data** and you need to be sure you are processing this lawfully. You also need to look at who in your group or organisation processes or uses personal data and make sure they comply with your Policy and with the requirements of the Data Protection Act 1998.

You might already be handling some of these well enough. Or you might find you need to change or add to some of the things you do.

Quick Glossary on Data Protection

Data Controller: Anybody (a person or an incorporated organisation) who decides what personal data to collect and how to process it. (In the case of voluntary and community groups, the management committee will share this role.)

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

Data Protection Compliance Officer: The person in your organisation who makes sure you comply with the Data Projection Act 1998.

Notify: Has replaced “Register”.

Data Processing: From the moment you take someone’s details to the moment you shred or delete their file, you *process* data about them.

Personal Data: Any information about a living person could be personal data, from name and phone number to family history and financial details.

Sensitive Data: The Act defines certain types of information (e.g. about medical issues; religion; membership of Trade Unions) as sensitive and there are special rules to follow.

Further information

This handout can only give you a very general idea of the things you might need to do to get started with Data Protection. It is not intended as a complete statement of the law. You should take advantage of the following sources of information to find out all that you need to know.

An excellent starting point is **Getting it Right: A brief guide to Data Protection for small businesses** and a simple checklist are excellent introductions published by The Information Commission. To find out whether or not you are a Data Controller, you can use **Notification Exemptions: A Self Assessment Guide**. This enables you to run through a checklist of basic questions to see whether or not you are a Data Controller and whether you need to notify. This guide is available as an online tool as well. The Information Commission also publishes the **Data Protection Notification Handbook: A complete Guide to Notification.**

You can also obtain the **Codes of Practice** from the Information Commission. Currently there are 6 Codes of Practice on CCTV; Recruitment and Selection; Employment Records; Monitoring at Work; Information about Workers’ Health; and Telecommunications Directory information and Fair Processing. Supplementary guidance to some of these codes is also available.

You can contact the Information Commission for all of these publications, or find them on their website under Data Protection. The Frequently Asked Questions section of their website is also very useful.

Information Commissioner's Office
www.informationcommissioner.gov.uk

Another very good introduction is the Institute of Fundraising **Code of Fundraising Practice on Data Protection.**
www.institute-of-fundraising.org.uk

Data Protection for Voluntary Organisations.
Paul Ticher. ISBN No 1 900360 47 0

This a guide written especially for voluntary and community organisations, and includes brilliant case studies to illustrate the practical reality of various points covered.
Cost £12.95 at time of writing, and is available from the Directory of Social Change, 24 Stephenson Way, London, NW1 2DP
020 7209 5151
www.dsc.org.uk

Hull CVS
'community and voluntary services'

Contact details

tel	01482 324474
fax	01482 580565
email	information@hull-cvs.co.uk
office	The Strand 75 Beverley Road Hull HU3 1XL
website	www.hullcvs.org.uk

Disclaimer

July 2010