A guide to data protection

nicva

A guide to data protection

Introduction

Data protection can seem like a very daunting subject for those not familiar with the jargon and legal terms. However, at its very core is the idea of managing information properly to protect individuals and their rights. This is an ideal to which organisations in the voluntary and community sector can easily relate and you may find that you are already complying with many of the requirements mentioned in this document anyway.

This guidance is based on knowledge built up over the past couple of years and is intended as a straightforward introduction to the subject of data protection. It is by no means an authoritative document and it would be impossible to cover every scenario but hopefully it will give you a starting point from which to build your knowledge.

If you have any comments or suggestions in relation to this guide please contact NICVA's Information Officer, Seána McAuley by email seana.mcauley@nicva.org or call 028 9087 7777

What is data protection?

The Data Protection Act lays out a framework for handling personal information, ie information about people. Data protection is about personal information not statistics. The Act gives individuals rights to protect their personal information and the right to privacy and places obligations on organisations to ensure they handle information fairly.

Personal data or personal information is any information that can be used to identify a living individual. It includes information such as a name, address, contact information, employment history, medical conditions, convictions, credit history. It can also include opinions expressed about an individual.

Sensitive data is information on racial and ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health, sexual life or criminal convictions / alleged offences.

You may see the following terms used when reading about data protection:

- **Data subject** – the individual who is the subject of the personal data
- **Data controller** – the individual or organisation who determines the purposes for which, and the manner in which, personal information is to be processed.
- **Data processor** - a person, or organisation, who processes personal information on a data controller's behalf.
- **Manual records/Relevant filing system** – Data protection applies to manual records that are held within a relevant filing system. This means that a filing system that is set up in such a way as someone going through the system could readily find personal information about someone. This could be employee records in a filing cabinet organised in alphabetical order and sub-divided into aspects of employment. But, if the files are only in alphabetical order and information is just put into the file with no further organisation then that is not a relevant filing system. Some good examples are given in the ICO's Technical Guidance Note on relevant filing systems.

The Data Protection Act 1998 came into force on 1 March 2000 and builds on the previous Data Protection Act 1984. The UK Act is based on EU Directive 95/46/EC. The 1998 Act covers personal data recorded in relevant filing systems and includes paper as well as electronic records.

The Act and use of personal information is regulated in the UK by the Information Commissioner's Office (ICO). The ICO can now impose fines of up to £500,000 if organisations break the law.

Processing/use of personal data must be carried out in accordance with the eight data protection principles. It should be:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept for longer than is necessary;
6. processed in line with your rights;
7. secure; and
8. not transferred to other countries without adequate protection.

These principles form the basic framework for anything you want to do with personal information. If in doubt consider what you want to do against these principles.

Why is data protection important?

- You are legally obliged to comply with data protection legislation
- It offers an opportunity to improve services and/or procedures
- It enables you to protect your service users' information
- It enables you to prevent harm
- It enables you to demonstrate respect for the individual
- It enables you to build trust with service users
- Handling the information you hold properly ensures it is an asset, not a liability.

How does data protection affect my organisation?

Do you have or do any of the following?

- Human resource information
- Redundancy and employment issues
- Service user / volunteer / staff information
- Photographs of service users / volunteers / staff
- CCTV images and video footage
- Sharing service user / volunteer / staff information
- Information security (systems, offices, transport, home working, disposal)
- Records retention
- Databases (management and accuracy)
- Direct marketing and promotional campaigns / newsletters
- Fundraising

If you answered yes to any of the above then data protection affects you and your organisation.

What can go wrong?

Data can be misused in various ways, it can be stolen which can harm the private interests of your organisation, it can be accessed by unauthorised people and used to hurt members of your organisation and it can be sold on to other companies for their own interests. In all these cases a fine of up to £500,000 can be imposed on your organisation by the Information Commissioner for allowing this breach to happen.

Examples of the harm caused by data protection breaches and the subsequent penalties vary on a case by case basis. In October 2012 the ICO fined its first charity. Norwood Ravenswood Ltd, a social care charity, was served a monetary penalty of £70,000 after highly sensitive information about the care of four young children was lost after being left outside a London home. The loss was deemed to be 'entirely avoidable' leaving the ICO with 'little choice' but to impose a fine. Read more.

There have also been some high profile breaches in Northern Ireland. Belfast Health and Social Care Trust was fined £225,000 following a serious breach at the vacant Belvoir Park Hospital site. The breach involved the sensitive personal data of thousands of patients and staff, and included medical records, X-rays, scans and lab results, and staff records including unopened payslips left at the site. The ICO's investigation found that the Trust failed to keep the information secure and also to securely destroy medical documents which it no longer required. Read more.

Data protection policies/procedures

Your organisation's data protection policy will be unique to its particular circumstances and will depend on the information it holds, what it does with it and the nature of the organisation. For some organisations a one page policy might be sufficient, while for others 20 pages may be necessary. In this case one size definitely does not fit all.

Before you write your policy you should consider carefully the information you hold, why you need it and don't keep any information you don't need. Apart from anything else it costs money to store extra information. Carry out an **information audit** – an audit of all the information your organisation holds, the reason you hold it and where it is stored. This is a useful way of identifying exactly what your organisation has and areas for improvement.

What to consider when creating your policy

Not all of the areas outlined below may be relevant for your organisation so if you don't have it or don't do it then you don't need to include it.

Responsibility
Data protection is an important element of every organisation's information strategy and as such it needs to be considered at senior management level. Staff should be aware of their responsibilities when handling information.

Write in plain English
There is no point going to the effort of writing a policy if no one can understand it. Write clearly, explaining concepts for staff/volunteers who perhaps aren't familiar with the terminology.

Electronic v paper
Remember to consider both electronic and paper files when writing your policy.

Information security
There are many simple ways to keep your organisation's information secure. Lock filing cabinets, password protect computers and mobile phones, checking email addresses and fax numbers before you press send, are just some examples.

Data must be kept as secure as possible which depending on the circumstances and resources of your organisation may include; password protection, encrypted files, limiting access to authorised individuals, training staff in proper protocols and proper filing/storage systems. For more advice on what security you should have please go to; http://www.ico.org.uk/for_organisations/data_protection/security_measures.aspx

Access
Consider who in your organisation has access to what information. Only people who need to have access should have access.

Storage
How is information stored? On computers, central file system, filing cabinets. Are these password protected or locked?

Transport
How is information transported? Laptops, bags, mobile phones, briefcases, notepads, case files, diaries, USBs. Are these secure and locked or password protected and encrypted? Are they left unattended? Are they taken home? What about break-ins? Think about all the ways you move information around and how it could be more secure.

Retention
Think about how long you need to keep information for. You might need to keep information for certain periods of time to meet legal requirements, ie financial documents, employment records, etc; you may need to keep it for funders; or you can decide based on the needs of your business. Think about why you need to keep it, the rationale for keeping it and explain this in a retention schedule. Create a retention schedule for your organisation and make sure your staff know about it so they don't keep information for longer than is necessary.

Disposal
How do you dispose of information when it's no longer needed? Do you employ a specialist document disposal company? Do you destroy old hard drives? How is any information used by staff working from home destroyed?

Processing information
To process information you need to meet at least one of the Data Protection Act's conditions for processing set out in Schedules 2 and 3. For non-sensitive information an organisation must meet at least one of the conditions set out in Schedule 2 listed below:

- The individual whose personal data it is has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

When processing sensitive personal information you must meet even stricter conditions, one of the conditions from schedule 2 **AND** one from Schedule 3 listed below. **Sensitive personal data** means personal data relating to an individual's race/ethnicity; religious beliefs; political opinions; health; sexual life or orientation; criminal convictions (or alleged convictions).

- The individual who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.

- The processing is necessary to protect the vital interests of:

  - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or

  - another person (in a case where the individual's consent has been unreasonably withheld).

- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

If you are unsure about how your use of information meets the criteria above contact the Information Commissioner's Office for specialist advice.

Read more about processing information and the conditions at http://ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing

Collecting personal information/getting consent
This is an essential task to enable you to collect and use personal information. As a rule you must get consent from users to process their information. Consent may be verbal or written. You must be clear about why you want to collect that person's information and what you will use it for. You must provide a privacy notice or privacy statement to the individual; basically this is a 'how we use your information notice'. Again this can either be verbal or written. If you have concerns about whether or not your organisation has the correct consent you can contact the people involved to get permission or alternatively contact the ICO for specialist advice.

Privacy notices/statements
Getting consent to use personal information for your organisation's purposes is possibly the most important thing to get right. Getting consent gives you assurance that you can use the information for the purpose(s) you have stated. It is also reassuring for people to know why you want their information and what you will do with it. Remember that consent can be withdrawn at any time by an individual.

Consent can be a more difficult concept where you want to collect information from children/young people or vulnerable adults. From what age can children give consent? How do you judge someone's ability to give informed consent? If in doubt seek advice from the Information Commissioner's Office.

Consent is obtained by means of a privacy notice/statement. A privacy notice is a legal requirement in order to meet the first principle of the Data Protection Act which says that personal data should be fairly and legally processed. Most of you will have agreed to one of these. If you shop at Amazon, use Facebook or iTunes you will have agreed to a privacy notice before being able to log in to the site.

A privacy notice should tell people at least who you are, what you will do with their information and who it will be shared with. A privacy notice can be verbal or written. You can find out more in the ICO's Privacy notices code of practice.

Databases
Whether your organisation's database(s) is large or small, the principles are the same. It is a legal requirement that the personal information held within your database is kept accurate and up to date in order to satisfy the fourth principle of the Data Protection Act. Aside from the issue of data protection, incorrect information is worthless to your organisation.

So long as consent is gained from individuals who know what you plan to do with their data, you can share their data with other organisations according to your data sharing agreements.

Human resources
Organisations with employees will hold a large amount of personal information, including sensitive information. You will have contact information, financial details for payroll, and possibly medical information. You may even have disciplinary, redundancy or pension information. There are specific periods of time you legally need to hold information for which can be found on the CIPD website at http://www.cipd.co.uk/hr-resources/factsheets/retention-hr-records.aspx.

Employees also have the right to make subject access requests for the information you hold on them. For more details guidance on human resources implications download the ICO's Employment practices code.

Fundraising
The Institute of Fundraising has issued a Code of Fundraising Practice which NICVA recommends fundraisers follow. The code has guidance on data protection issues relevant to fundraising practice available at http://www.institute-of-fundraising.org.uk/guidance/code-of-fundraising-practice/

Marketing
The rules for direct marketing (unsolicited marketing, ie addressed to an individual but which has not been requested) are quite strict and regulated by the Privacy and Electronic Communications Regulations (PECR). The ICO has published guidance for charities on what they can and can't do in terms of marketing. Key to the regulations is that it is an offence to send unsolicited marketing by electronic mail, text, fax, etc without consent.

The Data Protection Act gives individuals the right to stop their information being used for marketing purposes and you must comply with this.

However if an individual would reasonably expect to receive marketing material from you consent can be implied. For example, if someone attends a training session you are running they might reasonably expect that you would send them information on

other training sessions offered. Always include a way for the individual to "opt out" whether that is a contact name, email address, telephone number, etc. Remember that if someone objects/opts out you should remove them from your list as soon as possible.

Read more in the ICO's guidance:

Charities and marketing

Guide to the Privacy and Electronic Communications Regulations

Sharing information
You must take caution when sharing other people's personal information. Generally speaking you can release any information that is already in the public domain, for example, a charity worker's contact details available online. And, of course, you can share information as long as you have consent to do so from the individual. Any data sharing needs to consider the impact it will have on the individual.

In some circumstances you may wish to share information you have collected with third parties. For example, your organisation may outsource payment of staff to another company. This activity involves sharing employees' personal information and should be covered by a data sharing agreement. Another example might be where your organisation is working in partnership with another organisation (charity, statutory, private) to deliver services. If this involves sharing personal information of service users then you must make sure a data sharing agreement is in place.

In some cases, particularly where your organisation is working in partnership with the health service or a government department, there may be a standard set of procedures and an agreement to follow.

Data sharing agreements
Data sharing is where organisations agree to share their data with each other. The agreement is the set of rules stating how they will share their data. This should be considered on a case by case basis as the circumstances may be different each time you want to share data. Make sure that in any agreement you cover at least these important points:

- The reason why you are sharing data and the purpose of the data
- Who will get the data and how it will be secured
- What the data is (this may need to be quite detailed depending on the types of data involved)
- The basis for sharing – you need to give an explanation of the authority under which you are sharing information (consent, legal requirement, etc)
- If they get to keep it or delete it after a certain period
- What to do if an organisation receives a request for access to data.

Much more detailed information on data sharing is available in the Data sharing code of practice.

Cloud computing
Many of you will already be using the cloud either professionally or personally. Google docs, Hotmail, Microsoft 365, etc are all examples of services hosted in the cloud. If your organisation stores personal information in the cloud you are ultimately

responsible for its security. You must check your contract with your provider and receive assurances about the location and security of your information. Ensure that you have appropriate safeguards in place by checking the provider's confidentiality agreement and data protection policy. More in depth guidance can be found in the ICO's Guidance on the use of cloud computing.

Websites
For many organisations, their website will be a vital point of contact with individuals. You should include a privacy notice on your website (see NICVA's) to tell people what your organisation does with their information. This is also a good way to be open and transparent about the way your organisation manages information.

Cookies
There has been a lot of media coverage about cookies but what exactly are they? Cookies are small files stored on the hard drive of your computer and are used by website for various purposes. They can be used to allow a website user to log in to a site, to make the web user's experience better (like when payment and delivery information is stored for future purchases) or to provide analytics to inform improvements to a website. So they aren't all bad.

Cookies got a bad reputation because some websites were, and are, using them gather excessive information on the cookies your website uses and what they are for. Legally you are required to have some kind of visible notification that your website uses cookies by having a banner, pop up, etc. This can be used to obtain implied consent by saying something like 'by continuing to use this website you are giving permission for cookies to be set on your computer'. If you are unsure if your organisation's website uses cookies contact the person who created your website.

Photographs/images
The Data Protection Act does not prevent you taking photographs at events. Images of an individual are, however, considered to be personal information so although you can take photographs you need consent to use them. It is particularly important to consider how you will get consent to use images from children/young people and vulnerable adults. You can create a release form for individuals to sign explaining what you will do with the photographs, ie for use in printed and electronic media, including the internet, for promotional purposes and for addition to the organisation's archive.

Alternatively you could choose to give people prior warning as NICVA does in event registration emails to give them plenty of time to voice any problems, eg 'NICVA may take photographs/video/sound recordings at this event for use in printed and electronic media, including the internet, for promotional purposes and for addition to NICVA's Archive. For more information please read our privacy notice www.nicva.org/privacy or contact NICVA's Information Officer at info@nicva.org'.

You might also give a verbal warning at the start of any event to say that photographs may be taken for use on the website/printed material and that anyone who does not wish to be photographed should make themselves known to the event organiser.

Photographs should be handled like all personal data and should be stored securely.

CCTV
Since CCTV can be used to capture images (which are personal information) it falls under data protection. You must provide a privacy notice which may look something like this

The notice should be clearly visible. Footage can be divulged to the police for the purposes of prevention or investigation of a crime. Footage should also be disclosed to individuals as part of any subject access request. Further advice can be found in the CCTV code of practice.

Staff and volunteer training
Training of staff and volunteers is a crucial method of improving information security and thereby complying with the seventh principle of the Data Protection Act (Personal information must be secure). Ensure that all staff and volunteers are aware of the importance of handling information properly, that they need to be careful when using personal information, and to follow the organisation's procedures at all times.

A useful training checklist is available on the ICO's website.

Subject access requests
The Data Protection Act gives power and rights to individuals. Everyone has the legal right to know what information an organisation holds on them and to amend/correct the information if it is wrong. Requests must be made in writing (letter, fax, email) and organisations must reply to requests within 40 calendar days. Organisations can charge a fee of up to £10 to process a subject access request or up to £50 in the case of educational or medical records. You should consider how you will confirm the identity of the person making the request and how to protect the privacy of any third party individuals whose information may also be included in the records. Procedures for handling subject access requests should be clear to staff: who handles them, who collects the information, and who authorises them. There is a useful Checklist for handling requests for personal information (subject access requests) on the ICO website and a new Code of practice has just been issued.

If the request is likely to lead to a third party being identifiable from the information you must take extra steps before releasing the information. Where possible delete or black out that information; where this is not possible or someone could still be identified indirectly then you must either obtain the third party's permission or seek advice from the ICO on a case by case basis on whether the request is reasonable or not. More information is available in the ICO's technical guidance note on Dealing with subject access requests involving other people's information.

Notification

Notification is the procedure by which organisations using personal information register with the ICO. It is a legal requirement for any organisation processing personal information to notify the ICO but an exemption does exist for most charities. Some charities choose to notify voluntarily as it is a useful way to show funders and public sector contractors that you have tackled the issue. You can check to see whether or not you need to notify using the self-awareness tool online at http://ico.org.uk/for_organisations/data_protection/notification/need_to_notify or contact the notification team helpline on 0303 123 1113 or email notification@ico.org.uk. NICVA has notified and you can search for its registration at http://www.ico.org.uk/what_we_cover/register_of_data_controllers

Reporting breaches

If your organisation does suffer a breach of information security and loses or has personal information stolen it is good practice to report the breach to the ICO. There is no legal obligation to report a breach but any investigation by the ICO will take into account any action taken by the organisation. In other words it is in your organisation's interests to tell the ICO upfront. If you need to report a breach go to the Information Commissioners Website and download the Data security breach notification form:

http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Mergers and partnerships

Working in partnership and sharing information between organisations is becoming more common within the voluntary and community sector. Government policy and funding bodies increasingly advocate collaborative working to deliver services yet sharing information between organisations carries inherent risks.

Mergers and partnerships can result in the sharing or acquisition of personal information. You should be particularly careful about consent and sharing issues. Who owns the information? Whose responsibility is it to make sure the information is used properly and stored/shared safely?

If you are concerned about this issue or would like specialist advice on mergers and partnerships or any kind of collaborative working contact CollaborationNI on 028 9087 7777, visit www.collaborationni.org or email Project Coordinator Leeann Kelly at leeann.kelly@nicva.org.

Volunteers

Volunteer involving organisations can potentially hold a range of personal information on volunteers. The type and quantity of personal information that an organisation holds on a volunteer will depend on the nature of the role and the frequency and intensity of the activity.

Volunteer Now has developed an information sheet setting out some of the possible 'operational' and 'regulatory' reasons for holding different categories of personal data on volunteers. It also lists some of the things organisations might want to take into consideration when determining the length of time they keep certain pieces of information.

The Information Sheet is available from the Volunteer Management Section (under Legal Issues) of the Volunteer Now website.
http://volunteernow.co.uk/fs/doc/publications/retention-of-volunteer-data-info-sheet.pdf

For further information please contact Christine Irvine, Senior Policy and Information Officer by email christine.irvine@volunteernow.co.uk or call 028 9081 8332.

Further reading

Other resources you may find useful include:

Protecting data, protecting people: a guide for charities (2013). Charity Finance Group.
http://www.cfg.org.uk/resources/Publications/~/media/Files/Resources/CFDG%20Publications/Data_Protection2013.ashx

Data protection (2004). Lasa computanews guide.
http://www.lasa.org.uk/uploads/publications/ictpublications/computanews_guides/lcgdp.pdf

Data protection policy template (2008). Lasa.
http://www.ictknowledgebase.org.uk/fileadmin/ICT/rtf/Data_Protection_policy_template.rtf

Information Commissioner's Office

Advisory visit – the ICO offers a free, one day informal visit looking at security, records management and subject access requests. They are a good opportunity to get expert advice on areas for improvement. To register your interest in a visit http://www.ico.org.uk/for_organisations/data_protection/working_with_the_ico/advisory_visits

ICO advice
The ICO recently looked at the main topics which emerge time and time again with organisations they come into contact with. The top five areas for improvement are:

1. Tell people what you are doing with their data.
2. Make sure your staff are adequately trained.
3. Use strong passwords.
4. Encrypt all portable devices.
5. Only keep people's information for as long as necessary.

Next steps

Data protection, what do you need to do?

1. Ensure data protection policies are in place and up to date
2. Restrict access to personal data
3. Identify a senior level individual to act as senior information risk owner
4. Continually make staff aware of the existing information governance policies and guidelines
5. Secure data internally and externally
6. Develop data protection within homeworking and IT policies
7. Maintain a retention and destruction schedule
8. Be aware of changes to Privacy and Electronic Communications Regulations.

Northern Ireland Information Commissioner's Office

3rd Floor, 12 Cromac Place,
Gasworks
Ormeau Road
Belfast
BT7 2JB

t: 0303 123 1114
e: ni@ico.org.uk
w: www.ico.org.uk