



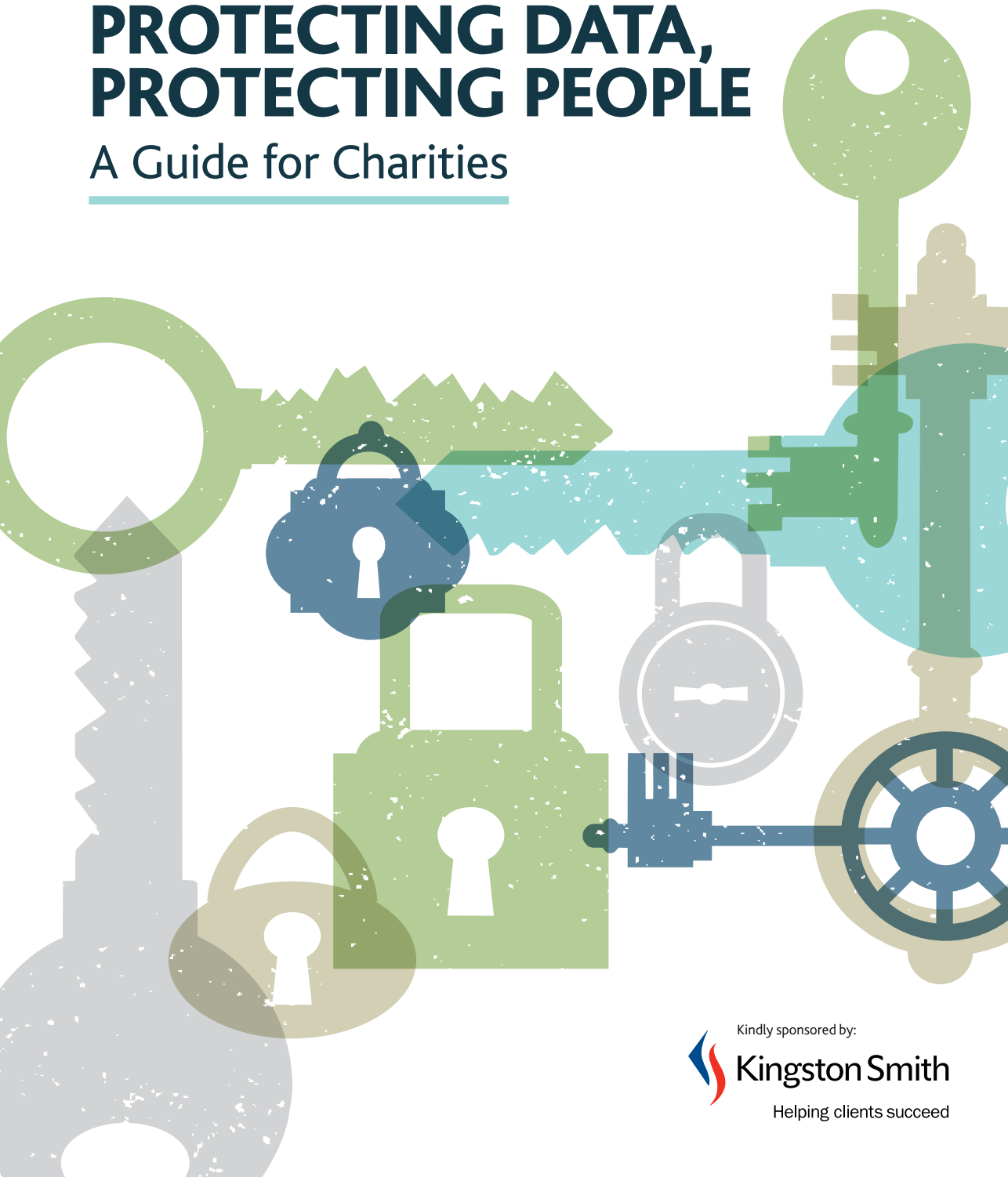
INSPIRING
FINANCIAL
LEADERSHIP

Produced in collaboration with:

BWB
Bates Wells Braithwaite

PROTECTING DATA, PROTECTING PEOPLE

A Guide for Charities



Kindly sponsored by:

 **Kingston Smith**
Helping clients succeed

April 2013

Material is contained within this publication for which publishing permission has been sought and for which copyright is acknowledged. Permission to reproduce this material cannot be granted by the publisher and application must be made to the copyright holder.

Every effort has been made to ensure the accuracy of the information contained within this publication.

However, the copyright holders cannot be held responsible for any action an individual or organisation takes, or fails to take, as a result of this information.

This publication has been produced in collaboration with Bates Wells and Braithwaite and Kingston Smith

The guide has been written and produced by the Charity Finance Group. Special thanks go to Jazmine Bradfield for project managing and drafting the guide, to Mairead O'Reilly and Lawrence Simanowitz from Bates Wells and Braithwaite and to Paul Ticher for their technical assistance. The production of the guide was supported by a steering group of CFG members and subscribers to whom we are very grateful. Steering group members were:

- Carolyn Collard, Glyndebourne
- Ben Willbond, Nuffield Trust
- Dominic Newton, Action for Children
- Michael Waterson, Conciliation Resources
- Judith Spencer Gregson, Muscular Dystrophy Campaign
- Paul Ticher, Independent Consultant
- Mairead O'Reilly, Bates Wells and Braithwaite

Other contributors whose input is much appreciated include:

- Information Commissioner's Office
- John Elford, BBC Media Action
- Rowenna Fielding, Alzheimer's Society

ISBN: 978-0-9567860-3-6

What is data protection about? – Protecting people

Simply put, data protection is about protecting people from the misuse of their personal information.

Data protection legislation aims to prevent harm to those individuals we process data about by creating legal responsibility for keeping the information we hold as safe as possible. In order for the charity sector to operate effectively, vast amounts of personal information must be held by charities. Fundraising, for example, is a vital operation for many charities, for which collecting information to build and expand a list of supporters is a perfectly legitimate objective. However, in order to prevent harm to those supporters, we need to ensure this information is not misused, does not fall into the wrong hands and that (where appropriate) individuals consent to their information being used in this way.

Why is data protection important for charities?

Not only is there the potential for the imposition of a civil monetary penalty or other enforcement action from the Information Commissioner's Office (ICO), but the potential for reputational damage to charities is huge. The voluntary sector depends upon the trust of the public, but it is difficult to ensure we're 100% secure at all times. Therefore it is important for charities to be able to demonstrate that they are aware of their responsibilities to keep the data they hold secure, and that they are taking proportionate measures to protect personal data from misuse.

Data protection may sometimes be seen as an issue for organisations with large databases of thousands of supporters or service users, but even the smallest organisations are likely to hold personal data on people such as staff or trustees. These organisations, which often rely on their existing reputation, can stand to lose just as much from a breach as those who spend millions on IT, if not more. It is vital that all organisations periodically review their policies and procedures around data protection and ensure that they remain 'fit for purpose'.

Contents

5	ABOUT THIS GUIDE
5	1.1 - What is this guide for?
6	1.2 - Who is this guide for?
6	1.3 - How should this guide be used?
7	UNDERSTANDING THE BASICS
7	2.1 - Where does data protection law come from?
7	2.2 - What does the Data Protection Act say?
8	2.3 - Do I need to notify the Information Commissioner's Office?
9	2.4 - Data controllers and data processors
9	2.5 - What is personal data?
12	2.7 - What is sensitive personal data?
13	WHERE TO START? HOW TO APPROACH DATA PROTECTION
13	3.1 - Data protection as a risk based exercise
14	3.2 - Steps to take in developing a data protection policy
15	3.3 - Deciding what information to collect
15	3.4 - Best practice
16	3.5 - ICO audits

17	THE PRINCIPLES
17	4.1 - Principle 1. Handling data fairly and lawfully
21	4.2 - Principle 2. Obtaining and processing data for specified and lawful purposes only
29	4.3 - Principle 3. Ensuring data is adequate, relevant and not excessive
35	4.4 - Principle 4. Ensuring data is accurate and up to date
37	4.5 - Principle 5. Retaining personal data
43	4.6 - Principle 6. Rights of individuals
51	4.7 - Principle 7. Information security
59	4.8 - Principle 8. Transfer of data abroad (outside the EEA)
69	OTHER THINGS TO CONSIDER
69	5.1 - Credit cards
69	5.2 - Enforcement & penalties
71	5.3 - Bring your own device
71	5.4 - The cloud
77	6.1 - DATA PROTECTION CHECKLIST

COMMON QUERIES FROM CHARITIES	PG
Do we need to notify the ICO?	8
What are the rules around requests for personal information?	46
What do we need to know when carrying out a charity's marketing activities?	47
How do we keep our data and information secure?	51
What do we need to know as an employer?	72
What do we need to know if we outsource our pay-roll, direct mail or other function?	72

CASE STUDIES	PG
Conciliation Resources: using contact data for "specified and lawful purposes"	25
Action for Children: ensuring personal data is "adequate, relevant and not excessive"	31
The Nuffield Trust: ensuring the security of personal data	53
Charity X: transferring data abroad	64
Glyndebourne: credit card security	73

About this guide

1.1

What is this guide for?

Data protection can be a challenging area of law to negotiate. This guide explains each of the data protection principles and provides examples of the issues you should be considering when creating, reviewing or implementing a data protection policy.

Often when people think of data protection, they first think about preventing the loss of laptop computers or restrictions on contacting supporters or other contacts, but there is much more to it than that. This guide works through each of the data protection principles in turn, with chapters at the end on enforcement measures and some of the other issues to be aware of when ensuring your organisation is compliant.

Data protection law derives from European privacy law. As such, it can appear vague and confusing where it concentrates on the principles by which decisions should be made rather than listing specific requirements. There are strengths to this approach however, which is generally concerned with "striking the right balance". This means that, whilst you must ensure your organisation complies with the principles, there can be some flexibility for you to decide upon an appropriate and proportionate way for your organisation to do so.

This guide should help you to determine the right balance for your organisation. A number of case studies have kindly been provided to illustrate the approach taken by some of CFG's member organisations in establishing the best way for them to work within a certain principle. These are focussed on the issues that the individual data controller must take into consideration in finding the right balance for them, and are intended to be illustrative for readers.

1.2

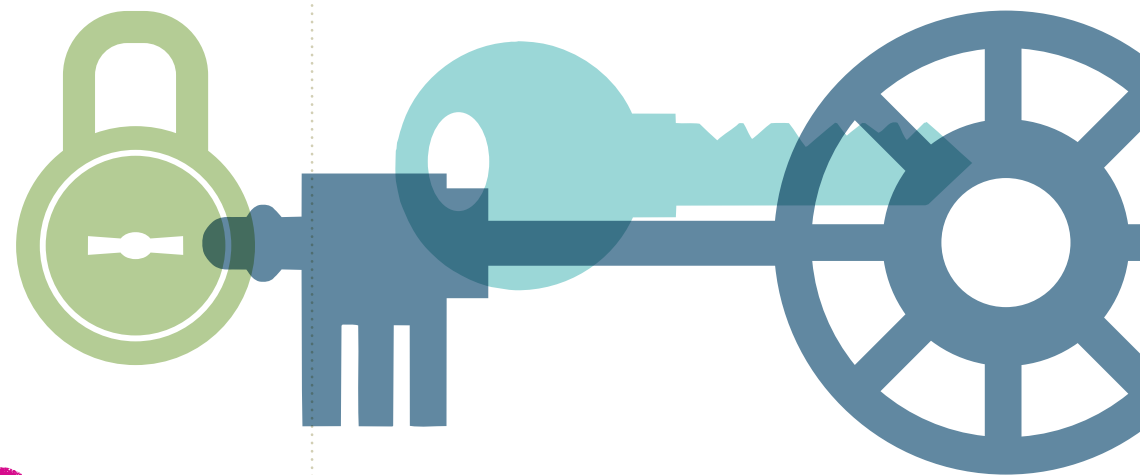
Who is this guide for?

This guide is intended to enable the person responsible for ensuring data protection in a charitable organisation to review their data protection procedures, identify weak spots and decide on appropriate measures to remedy them. It is aimed at the person responsible for their organisation's data protection policies and to help inform decisions about the necessary components of their data protection regime (e.g. staff induction, training and supervision).

1.3

How should this guide be used?

This guide, having taken into account the different ways in which the charity sector works, aims to help you understand what the law on data protection means for your charity. A vast amount of more general guidance already exists on data protection and it is not the intention to replicate it here. CFG has worked with the Information Commissioner's Office (ICO) (the body responsible for ensuring data protection compliance in the UK) to bring their best practice notes to your attention, in addition to a number of other useful resources which will provide you with further information.



Signposts: Wherever you see this symbol at the end of a paragraph, the accompanying footnote will direct you to further information. This may be from the ICO or another freely available source.

Key questions: Each section in the chapter on principles contains key questions. These questions are the very minimum you should be asking of your organisation and are based on the ICO's checklist for small businesses. Being able to answer 'yes' to all of the questions will not guarantee compliance, but will demonstrate that you are heading in the right direction. A full checklist of these questions can be found at the back of the guide.

Understanding the basics

2.1

Where does data protection law come from?

The Data Protection Act 1998 (DPA) came into force on 1st March 2000 and comes from the European Data Protection Directive; part of the European Union's body of privacy and human rights law. The DPA regulates the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The Privacy and Electronic Communications Regulations first came into force in 2003 and include provisions relating to electronic marketing which may also have implications for your data protection policy and practices. These regulations were updated 2011 and include new rules on the use of cookies on websites – you should make sure your website is compliant by checking the ICO guidance.

2.2

What does the Data Protection Act say?

The DPA places obligations on organisations that process personal information and gives individuals certain rights.

The DPA states that those who record and process personal information must be transparent about how the information is used and must follow the eight principles of "good information handling" which are contained in schedule 1 of the DPA.

The eight principles can be summarised as follows:

- a. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
 - at least one of the conditions in Schedule 2 is met, and
 - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.



More information can be found on the ICO website covering:

- Notification
- Not-for-profit exemption

- b. 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.
- c. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- d. Personal data shall be accurate and, where necessary, kept up to date.
- e. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- f. Personal data shall be processed in accordance with the rights of data subjects under this Act.
- g. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- h. 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.

2.3

Do I need to notify the Information Commissioner's Office?

Almost all organisations that act as data controllers must register with (notify) the Information Commissioner, giving details on the types of data they hold and the purposes for which they are processing personal data. This notification must be renewed each year. Fees operate on a two-tiered system and the fee you pay is determined by the size and income of the organisation. All registered charities pay the lower tier fee of £35. Other organisations can pay the lower tier fee of £35 unless they have a turnover of more than £25.9m and have more than 250 members of staff, or are a public authority with more than 250 members of staff.

There is an exemption from the requirement to notify for 'not-for-profit' organisations but it is very narrow and charities must satisfy certain conditions in order to rely on it. It is possible that very small charities, or those with very limited operations may meet the criteria, but as a matter of best practice it is recommended that if in doubt, you notify.

For more information on notifying the Information Commissioner, see page 24.

2.4

Data controllers and data processors

The Data Protection Act 1998 defines these terms as follows:

"Data controller" means a person who determines the purposes for which and the manner in which any personal data are, or are to be processed;

When the data protection officer, or other responsible employee within a charity, fills out the registration form for the ICO they must name the data controller. It is important to remember that although you may have a designated individual who is responsible for ensuring compliance such as a data protection officer, it is the organisation that is the data controller.

As a matter of best practice then, to avoid pinning unnecessary responsibility on an individual staff member it is always preferable to name the organisation as the data controller and not the organisation's data protection officer, regardless of the status of the organisation. This is also more factually accurate since it is the organisation and not an individual member of staff which is likely to be the data controller in reality, and will make the decisions on how personal data is handled.

"Data processor", in relation to personal data, means any person (other than an employee of a data controller) who processes the data on behalf of a data controller.

A data processor is anyone who processes data for and on behalf of a data controller, who is not an employee of the data controller. This could be, for example, a mailing house, a data destruction company, or a fundraising contractor making calls on behalf of the data controller. This means staff, volunteers, contractors and temporary staff are not classified as data processors. Under the DPA, a data controller is liable for what a data processor does with personal data processed on the data controller's behalf.

2.5

What is personal data?

The DPA is only concerned with the treatment of personal data. If information (data) relates to a company and not an individual it is not personal data and does not fall with the remit of the DPA. Similarly, although information that is personal but is not recorded anywhere (e.g. unrecorded conversations with service users) should be covered by your confidentiality policy, it will not fall within the DPA. In order to be 'personal data' for the purposes of the DPA information must meet the following conditions:

- 1. must be data; and
- 2. must be personal

	Personal About identifiable, living, individuals	Not personal About companies or people who are not identifiable or no longer living
Data Recorded either electronically, on a computer or manually on a relevant filing system	Covered by the DPA	Not covered by the DPA but you may have other reasons not to disclose it (e.g. in order to keep it confidential) which should be considered in your confidentiality policy
Not data Information which is not recorded or does not meet any of the criteria in section 1(1) of the DPA (e.g. unrecorded conversations with service users).	Not covered by the DPA but should be covered by your confidentiality agreements	Not covered by the DPA

¹It is worth noting that where a group or data set is small, a person may be identifiable. Even if their name or other information is not recorded it may be possible to identify the person from other characteristics which are known about them in the data set.

- Information is **personal** if it is:
- concerned with identifiable, living individuals
- Data** is information which is:
- a. processed by automatically operating equipment; or
 - b. recorded with the intention that it be processed by automatic equipment; or
 - c. recorded as part of a relevant filing system or with the intention that it should form part of one; or



More information can be found on the ICO website about:

- Personal data

- d. forms part of an accessible record as defined by section 68 (this includes health, social work and education records); or
- e. is recorded information by a public authority and does not fall within any of paragraphs (a) to (d).

Whether or not you have a relevant filing system (for c) can be determined by applying the "temp test". If a temporary staff member would, with ease, be able to extract specific information about a particular individual from a manual filing system without particular knowledge of the documents you hold, it may be regarded as held in a relevant filing system and therefore treated as data.

It is also important to be aware that photographs, videos etc that fall within any of the above categories can count as data if they are handled in one or more of the ways mentioned above.

WHAT KINDS OF PERSONAL DATA DO CHARITIES PROCESS?

Charities process a great deal of information. The kinds of information charities collect which may constitute personal data typically include:

- Job applications and CVs
- Payroll information
- Volunteers' details
- Members' details
- Case notes for service users, clients and other beneficiaries
- Personal information on donors
- Health information for staff, volunteers and trustees

2.6

What is sensitive personal data?

The DPA requires a higher degree of protection for sensitive personal data such as medical information or a person's criminal record because the potential for misuse of such data causing harm to the individual is much greater. The DPA lists the following categories of sensitive personal data:

- a. The racial or ethnic origin of the subject;
- b. The subject's political opinions;
- c. The subject's religious beliefs or beliefs of a similar nature;
- d. Whether the subject is a member of a trade union;
- e. Information on the subject's physical or mental health condition;
- f. Information on the subject's sexual life;
- g. The commission or alleged commission of an offence by the data subject; and
- h. Information relating to the commission or alleged commission of an offence by the data subject (i.e. the sentence of a court in relation to an offence).

Data controllers must satisfy additional conditions under the DPA in order to process sensitive personal data, more information on which can be found under Principle 1 on page 17.



How to approach data protection

3.1

Data protection as a risk based exercise

It is important that each organisation complies with the principles by adopting measures that are appropriate to their own activities and resources to minimise the risk that personal information will be misused.

This guide works through each of the principles, using case studies to highlight some of the issues you may need to consider when deciding on appropriate and proportionate measures within the context of your own organisation.

There are many different elements to data protection, and most people will naturally be more familiar with some aspects than others according to their job role. Someone who works in IT for example, is likely to think first of encryption and passwords, whereas someone who works in marketing will probably think of email lists and opt-in consents before information security measures.

Ensuring compliance with DP for most organisations will be about reviewing the activities of the whole organisation, identifying potential weak spots and taking steps to mitigate the resultant risks. The ICO recognises that it is not always possible to be 100% secure, but expects organisations to develop measures for protection that are proportionate to both their resources and the likelihood of harm to individuals.

3.2

Steps to take in developing a data protection policy

1. The first stage of this process is often described as an audit. Below are examples of the questions you should be asking in order to understand how the activities of your organisation may impact on your data protection policy.

- a. What information do you process?
- b. Does the information constitute personal data?
- c. Do you have a data protection policy?
- d. Do staff know how to find the data protection policy?
- e. Are staff trained in data protection?
- f. Who is ultimately accountable for data protection compliance?
- g. What other policies of the organisation may be affected by data protection?

2. The second stage of the process is to work through each of the principles and other considerations, across the whole of your organisation in order to determine any weak spots.

3. Once weak spots have been identified, the appropriate measures to address them should be adopted using a risk based approach. The likelihood of harm (the potential for which influences the likelihood of enforcement by the ICO) should be considered, as should the capacity of your organisation to prevent that harm.

- a. The importance of getting buy-in from all staff should not be underestimated throughout this process, as in order for each review to be effective staff must be honest about the data they use to do their jobs, and how they use it.

Whilst the data controller (usually the charity) is ultimately responsible for compliance and any penalties or undertakings will be addressed to them in the event of a breach, every employee or volunteer who is responsible for processing data should also be made aware of their role in adhering to the policies and guidelines of their organisation.

- b. As data protection compliance requires organisations to assess risk, your priorities should be those areas which present the highest risk of causing harm to those whose personal data you hold. The vast majority of monetary penalties have been issued in cases where personal data that has ended up in the wrong hands due to poor procedures or lack of awareness of the importance of data security. Common scenarios include the loss of unencrypted laptops and misplaced manual files which hold sensitive personal data.

3.3

Deciding what information to collect

There are a couple of things to be aware of when deciding what data your organisation should collect. A proportion of the personal data you hold will be necessary for the successful running of the organisation (HR records, case notes etc) whereas you will choose to collect some data in order to achieve your aims (supporters' information for example).

Although you will need to comply with all 8 principles, you should pay particular attention to principles 2 and 3 when deciding what information to collect. Although it may be tempting to collect every piece of information you feel may be useful one day, you should ensure you can demonstrate that the information you have collected is relevant, not excessive and is adequate in relation to the purposes for which it will be processed. Those purposes must also be specified to the data subject in a fair processing notice and to the ICO in your notification, and of course must be lawful.

3.4

Best practice

This guide has been drawn up around the experiences of CFG members. A number of case studies have been provided – and here those contributors have explained how they ensure compliance with the data protection principles, in their own organisations.

"The thing that worked for me was getting senior management buy-in – once they understood the potential for reputational damage if we got data protection wrong they no longer saw it as obligatory box-ticking and were incredibly supportive towards making necessary changes across the organisation."

'One of the biggest challenges for us as a large and geographically-diverse organisation is communication of training and awareness material to all levels of the organisation. While awareness and appreciation of the benefits of data protection has been at a high level for a long time, this did not necessarily correspond to understanding of how to apply the data protection principles in practice. A series of training sessions entitled "How to NOT cause a breach" were delivered using web-conferencing technology, allowing all levels and areas of our charity to be reached. This training, based on anecdotes, analogies and "what if" scenarios as well as practical advice was very successful in closing the gap between abstract awareness of the important of data protection and knowledge of how to apply good practice to everyday tasks.'

TERMINOLOGY

The following terminology will be used throughout the guide:

Notification: The process of registering your organisation with the ICO as a data controller

Data controller: The organisation that determines the purposes for which personal data is processed.

Data processor: Any external organisation or individual that processes personal data on behalf of a data controller.

Data protection officer: Whilst the organisation (as the data controller) is ultimately responsible for data protection it is good practice to nominate a data protection officer who will be responsible for developing and renewing the organisation's policies and ensuring new staff and volunteers follow them. This will usually be the person whose contact details are given on the notification.

Data subjects: Refers to any individual your organisation processes personal data about. This may include current and former staff, volunteers and applicants as well as your service users, donors and individuals in your fundraising database.

3.5

ICO audits

As charities often handle extremely sensitive data, the ICO are offering free one day advisory visits to charities to discuss and receive practical advice aimed at improving data protection practices. The visits last one day and each organisation is provided with a short report summarising the ICO's findings and providing practical advice on how they can improve. To request a data protection audit, visit the ICO's website.

EXPERIENCE OF THE ICO AUDIT: ALZHEIMER'S SOCIETY

In summer 2012, an arrangement was made between the Information Commissioner's Office and Alzheimer's Society for a consensual audit of data protection to be conducted, covering information security and records management. With the introduction of a new cloud-hosted Computer Records System, we were keen for the ICO's viewpoint on the work that had been done to ensure the privacy and security of the information in the system.

To help the audit team decide where to focus their attention, we were asked to provide copies of our policies, procedures and training material before the audit. This was no problem for us, as we had spent the preceding year developing an Information Governance Framework which brought all of this material together.

The auditors arrived in a small team - three people on the first day, then two auditors for the next two days. Over the three-day audit period, the team spoke to various people in the organisation who are involved in processing personal data, as well as visiting some front-line service delivery locations and talking to the organisation that provides IT services for the Society. The main focus was on the highly sensitive and confidential personal data that the Society needs to process in order to deliver services for people living with dementia - both ourselves and the audit team were keen to ensure that this information was being handled securely and appropriately.

Once the audit interview were over, we received the report and were pleased to note that the risk assessment we had conducted on using a cloud provider for our Computer Records System was cited as an example of good practice. The recommendations made by the audit team corresponded to areas of improvement which had already been identified by us and planned for as part of the ongoing work for the Information Governance Framework - there was nothing we'd missed or which took us by surprise. We found the experience to be extremely valuable.

Principle 1:

Handling data fairly and lawfully

4.1

The DPA says:

'Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- a.** at least one of the conditions in Schedule 2 is met, and
- b.** in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'

The first data protection principle is concerned with ensuring you process individuals' data fairly. Therefore you must:



1. Ensure you process data fairly.

Fair: In meeting the requirement to process data fairly you should predominantly be concerned with ensuring that you tell individuals how their personal information will be used in particular:

- Who you are;
- What you will use their information for; and
- Anything else necessary to ensure you are using their information fairly including whether you plan to pass individuals' details to other organisations and how you will contact people (i.e. by phone, post or email).



2. Ensure you do not do anything unlawful with the data.

For example, you may not be able to disclose information that was given to you in confidence.



3. Ensure that you can satisfy at least one of the conditions in schedule 2.

The schedule 2 conditions include the following:

- The individual who the personal data is about 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.

The "legitimate interests" condition may be satisfied if your processing is necessary for the purposes of legitimate interests. Typical examples where the "legitimate interests" condition may be satisfied include a finance company processing data by passing contact details on to a debt collector, or the processing of information about professional contacts in other organisations.



4. Ensure you have satisfied at least one of the criteria in schedule 3 if you process sensitive personal data (see page 12 for a definition of sensitive personal data).

- 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

Key questions: Do I really need this information about this individual?

Do I know what I'm going to use it for?

Have we met one of the schedule 2 conditions?

Do we process sensitive personal data? If so, have we met one of the schedule 3 conditions?

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

- The processing is carried out by some types of not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. This condition is quite restrictive and does not apply to most charities.
- 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.
- Processing to prevent or detect a crime where seeking consent would inhibit the ability to do so.

There are also several other rarely applicable criteria which apply in very specific circumstances. e.g. processing for journalism, counseling or pension schemes.

What does this mean for your data protection policy?



More information can be found on the ICO website about:

- Legitimate interests

In drawing up your charity's policy, you should review the purposes for which you wish to collect data and why. If the data you collect is personal you will need to satisfy one of the schedule 2 conditions and possibly a schedule 3 condition.

In many cases the most straightforward way to do so is to ensure you have the consent of the person the data is about. You will need to review the statement you make to people when you ask for their data and ensure that it:

- is clear and easy to understand;
- explains the purposes for which their personal data will be processed (examples of privacy notices can be found under principle 2);
- obtains their consent for processing where necessary.

Principle 2:

Obtaining and processing data for specified and lawful purposes only

4.2

The DPA says:

'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 second data protection principle is concerned with how you tell people what you will do with their data. There is a crossover with principle 1 as you cannot claim to process data fairly without explaining what you will process it for.

In practice, the second data protection principle means that you must:



1. Determine why you are collecting personal data and what you intend to do with it (your purposes).

Your purposes can be broadly defined, and one purpose can encompass several strands of activity. Typical purposes for which charities process personal data include employment, fundraising and marketing.

If you process personal data in order to communicate with supporters, potential donors or even people you want to persuade to sign a petition, it is important to be aware of the impact of the Privacy and Electronic Communications Regulations on how you contact individuals. The PECRs also contain rules about direct marketing, which the ICO defines broadly to include "a wide range of activities that apply not just to the offer for sale of goods or services, but also to the promotion of an organisation's aims and ideals".

This means that newsletters for example, or a call to action (regardless of whether it contains a financial ask) could be interpreted as marketing material. If you will use email addresses to send people information (such as newsletters or updates) which could be construed as marketing material you will need to specify this purpose in your privacy notice and obtain consent from the individuals you intend to contact in this way.

2. Ensure you give clear and accurate privacy notices to individuals when collecting their personal data. You should avoid using technical language. Phrases such as "how we use your information" are much more accessible than jargon.

In your privacy notice you should include:

- Who you are;
- The purpose/ purposes for which you will process their information;
- A consent statement if you intend to send the individuals marketing materials by email or text; and
- Anything else you need to include to ensure your processing of the information is fair such as who you may disclose the information to that the subject would not expect.

²(if you are not based in the UK you should say who your nominated UK representative is)

The important thing to consider is the likelihood of causing harm to the data subject by processing their data in a way which they did not expect. The format and exact wording of the privacy notice are less important than making it easy for people to understand what you will do with their information. The following examples have been provided by the ICO and can be found in their Privacy Notices Code of Practice.

Please provide telephone numbers in case we need to contact you about your claim.

You do not have to tell us your phone number but it will help us to contact you quickly if we have a question about your claim.

Home:	Work:	Mobile:
-------	-------	---------

Clear explanation of why it would be helpful to provide this information.

Using your personal information

1. Personal information which you supply to us may be used in a number of ways, for example: **a.** To make lending decisions **b.** For fraud prevention **c.** For audit and debt collection **d.** For statistical analysis

2. We may share your information with, and obtain information about you from, credit reference agencies or fraud prevention agencies. If you apply to us for insurance we will pass your details to the insurer. Information provided by you may be put onto a register of claims and shared with other insurers to prevent fraudulent claims.

3. We will not disclose any information to any company outside the XXXX Bank Group except to help prevent fraud, or if required to do so by law.

4. For further information on how your information is used, how we maintain the security of your information, and your rights to access information we hold on you, please contact: (clear weblink / freephone etc...)

Title that people will understand.

Clarity about who personal information is shared with and why.

Clear info about how to find out more. Easy, free access.

3. Notify the Information Commissioner.

Every data controller must state the purposes for which they process personal data in their notification to the ICO. The ICO provides standard purposes which you should use wherever possible. These include staff administration and advertising, marketing and public relations amongst many others. Below is an example how you would complete the form for provision of financial services and advice.

Purpose Example

Provision of financial services and advice

Data subjects are:

- Customer and clients;
- Complainants, correspondents and enquirers; and
- advisers, consultants and other professional experts.

Data classes are:

- personal details;
- family, lifestyle and social circumstances
- employment details;
- financial details, and goods or services provided

Recipients are:

- data subjects themselves;
- relatives, guardians or other persons associated with the data subject;
- business associates and other professional advisers;
- financial organisations and advisers, and
- Ombudsmen and regulatory authorities.

Transfers:

- none outside the EEA.

When reviewing your data protection policy, data collection statements (privacy notices) and or notification with the ICO you should:

1. Check whether you have specified all of the purposes for which you process personal data in your privacy notice and notification. If you need to add a purpose to your notification you can do so fairly easily, but you must be careful not to use data you have told people will only be used for a subsequent new and incompatible purpose for something else later on. It is better to encompass broader aims within your privacy notices such as "we will contact you with news and information we think will interest you" than to rule out, for example marketing purposes, then later decide you want to send a newsletter and risk damaging the reputation of your organisation when people are irritated at receiving information they did not expect to receive.

2. Be aware that it is important to ensure that people know what you are doing with their data. Whilst it may be tempting to comply with principle 2 by specifying your purposes only in your ICO notification, because you fear putting people off with a privacy notice, individuals are highly unlikely to look you up on the ICO's register before deciding whether to give you their details. You should see the privacy notice as an opportunity to demonstrate that you can be trusted and choose your wording accordingly.

Key questions: Have we told individuals how their information will be used?

Have we notified the Information Commissioner of the purposes for which we process personal data?

Is our notification up-to-date?

Are we clear internally what we have told people, so we know what purposes we can now use the information for?

Do we have/ want to have staff details on our website? If so, have we consulted with them?

Do we use CCTV? If so, are we displaying notices informing people that we are collecting information about them and are the cameras placed so as not to invade privacy?

Case Study

Conciliation Resources: using contact data for "specified and lawful purposes"

Conciliation Resources has been through a period of rapid growth and development during 2011 and 2012; this included a rebranding exercise, the creation of a new website and additional posts for a full time officer in the communications team. These factors provided the motivation and the capacity to revisit our communication strategies and practices in detail.

What personal data does Conciliation Resources process?

The new team inherited a custom-built database of contacts and a custom-built mass-mailing system. The contacts database had grown organically over more than a decade from being a shared address book with notes for a small staff team to becoming a large CRM database of over 20,000 records for a growing organisation. As a result of this organic growth, it was unclear which contacts had consented to receiving mass mailings and which had consented only to receiving individual emails from individual members of staff. There was an assumption of implied consent to receive mass emails if an individual gave their contact details to anybody at Conciliation Resources, but people could opt out of this and a note to that effect would be kept with their details.

How has the system changed?

As part of the launch of the new website, Conciliation Resources introduced a third-party mass-emailing provider, for news and information emails. Instead of being added to mailing lists by a Conciliation Resources staff member, interested parties subscribe to mailings through a page on our website that then populates the online email marketing system's mailing lists.

How did you merge the new and old systems?

While new contacts began to subscribe to mailings through the online email marketing system, around 7,000 existing contacts had been receiving news and information emails from Conciliation Resources but were only managed through the inherited contacts database. Our task was to ensure that we were using data (in this case, email addresses) in accordance with Principle 2 and would continue to do so in future whilst ensuring that existing contacts continue to hear from us if they want to.

It was important to give the existing contacts a clear opportunity to choose between continuing to receive Conciliation Resources mailings and unsubscribing from them. We sought legal advice and researched best practice guidance on how to proceed to ensure that Data Subjects had clear information and choice about the purposes for which we would use their data.

What was the transition process?

We began by adding features to our internal contacts database to record subscriptions and un-subscriptions to the online email marketing list through a regular import process.

We emailed (through the online email marketing system) the 7,000 existing contacts to explain what would happen:

"Title: Keep in touch with Conciliation Resources"

Dear <first name>

You're one of Conciliation Resources' valuable contacts and we don't want to lose you.

I'm getting in touch because we're changing the way we send out email bulletins (e-bulletins) about our work and news to comply with UK law. Whether you work in international peace building like us or simply have an interest in our peace building work, our e-bulletins help keep you informed about the important work we're doing to help resolve conflicts and achieve lasting peace.

You're receiving this email because you have previously shown some interest in our work. Given this, you have been added to our new system that will ensure you continue to receive e-bulletins from us.

If you want to continue receiving e-bulletins filled with our news and latest work, no action is required. If you would no longer like to receive our news via e-bulletins, please click on the 'unsubscribe from this list' link in the bottom section of this email. We'll be sorry to see you go!

If you'd like to make sure you receive e-bulletins with content specific to your area of interest, e.g. about our specific programmes, our policy work or job vacancies, please click on the 'update subscription preferences' link in the bottom section of this email.

The 'unsubscribe from this list' and 'update subscription preferences' links appear on every e-bulletin we send out, so you don't have to decide now if you don't want to.

Thank you for helping us comply with the UK's emailing regulations and I do hope we'll be sharing our latest peace building news with you soon."

A month after this email was sent we updated our contacts database to indicate those contacts who had subsequently unsubscribed. We then added the remaining contacts to our main (bi-monthly) news online email subscription list.

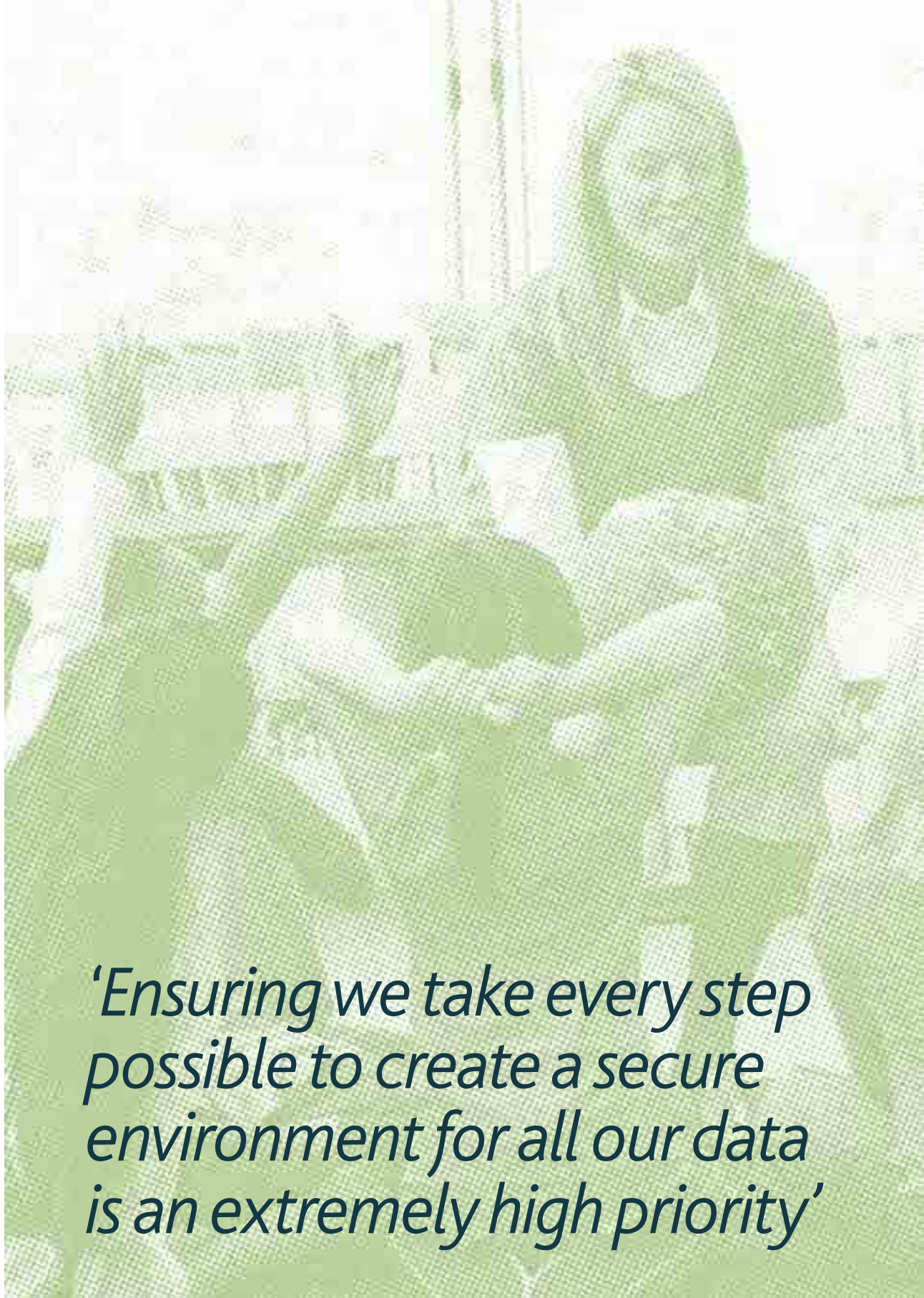
What is the current situation?

All recipients of Conciliation Resources news mailings are now managed through the online email system; contacts can be encouraged to subscribe to mailings by an individual staff member known to them, but can no longer be added to a mailing list without their explicit permission being recorded in the online email marketing database. Any subscriber/recipient of mailings can unsubscribe independently and with immediate effect.

Through monthly imports, our internal contacts database displays the mailing preferences set by the data subject in the online email marketing system.

What is planned from now?

Firstly, we are now reviewing our data protection and privacy policy to take into account our revised practices and best-practice guidance. Our contacts database will also be regularly and systematically reviewed to ensure that data is up-to-date and appropriate for the purpose for which it is held, and we are also working on ways to separate data about individuals from data about organisations.



'Ensuring we take every step possible to create a secure environment for all our data is an extremely high priority'

Principle 3:

Ensuring data is adequate, relevant and not excessive

4.3

The DPA says:

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'

The third principle is concerned with ensuring you hold the right information about your data subjects and no more than you require for the purposes for which you use it. Therefore you should:



1. Establish whether the information is relevant.

Review the categories of personal information your organisation holds, in order to decide whether each is relevant for the purposes you have specified in a privacy notice to the data subject and in your notification to the ICO.

It is important not to overlook those sources which you may not often need to use such as archived case notes, as it is those which are most likely to be superfluous to your requirements. Relevance should be your first consideration as holding information which is not relevant has implications for other principles. If you discover information which you feel is not relevant you should ask whether or not it is used by the organisation.

Do you use it?

If the answer is no – you should consider deleting it in accordance with principle 5

If the answer is yes – you should review your specified purposes (under principle 2) and consider adding the new one to your notification.



2. Establish whether the information you hold is excessive. If it is more than you require for your specified purposes you should delete it.



3. Establish whether the information is adequate to make the decisions it informs. Decisions which will have a significant impact on the data subject are likely to require a great deal of information and charities are often required to make those decisions.

Key questions: Is this information relevant to the way we process it?

Do we really need to have this information?

Do we have enough information to make the decisions we do?

Case Study

Action for Children: ensuring personal data is “adequate, relevant and not excessive”

What personal data does Action for Children hold?

Action for Children is one of the largest children's charities in the UK, providing a range of services to children, young people and their families. These include local authority commissioned children's centres, respite care, fostering and adoption projects and schools. We employ over 6,000 people at any one time and hold personal data on hundreds of thousands of individuals – reflecting our 143 years of history. As such, assessing adequacy and relevance is both very straightforward and very complex.

Why is data protection important for Action for Children?

Information is one of our largest assets and protection of it is one of our most important duties – we view ourselves as custodians with ethical as well as legal responsibilities to ensure it is handled and held properly. Ensuring that we hold the right information is vital both in making decisions, and protecting those who we hold information about.

How do you decide what is adequate?

Adequacy means very different things in our different services. Within highly regulated services such as fostering or residential care settings, we are required by statutory regulation to keep a minimum set of data, including detailed case notes, specific employee information and a range of non-specific records which hold personal data. This removes a great deal of the decision-making on adequacy for these services.

For our less-regulated provision however, there are two main drivers; the first being the requirements of our commissioners. In commissioning services such as Children's Centres, local authorities put in place various information requirements which generate a great deal of personal data. In large part this information is very basic; registration data on families accessing services for example, which provide quantitative data on the reach of the service. That said, in response to certain initiatives, specific information is sometimes required which we would not normally collect – data on stop-smoking services or breastfeeding support services for example.

Adequacy can therefore have a significant 'contractual' flavour in this type of service. Insofar as we are a data processor, this is not a problem; although drawing the line between processor and controller – and thereby seeking to limit the requirements on us from commissioners – can be a challenge.

What about your other services?

The second main adequacy driver across all of our services is to keep our service users safe. Our employees are regularly in the position of either having a safeguarding disclosure made to them, or otherwise having to raise concerns that lead to safeguarding referrals to a statutory agency. Ensuring that we have the correct level of relevant information to make those decisions is vital to our ethical obligations as a children's charity and the safety of our service users.

How do you decide what information is relevant?

In such cases (as has been proved across any number of Serious Case Reviews) what is relevant can be difficult to judge until after the fact. It is therefore tempting to record everything. However, it is more effective to train our employees to differentiate fact from opinion, ensure that sources of information are clearly identified and that, while personal judgements are of course necessary, they are a conclusion drawn from the information held and can be clearly understood – if not agreed with – by those they relate to.

A further complexity in this judgement is in ensuring that, where information is relevant, we have the right to record it. For example, if a parent/carer visits one of our services to pick their child up and shows signs of having been drinking, we may not have previously recorded any data about them; however an employee may now feel that it warrants recording in order to make a judgement as to whether a safeguarding referral needs to be made. This information is clearly relevant in terms of our duty to protect the child but we

are required to ensure that personal data is held fairly and lawfully – even though we do not always know in advance that we will need to record data on a specific individual.

So can you still record that information?

Because of these situations it is incumbent on us to ensure in our fair processing notices available to all parents and carers, that all data we deem relevant will be recorded – and this may include data relating to them.

What for Action for Children constitutes excessive data?

In many ways this is the most difficult aspect of our DPA compliance. Obviously not duplicating data is a factor, but limiting collection of data when working with families is a challenge; as noted above, it sometimes isn't clear what is relevant and what is not.

That said, there are some clear lines – it would not be expected for a Children's Centre to be maintaining detailed case-files on all service users, only those accessing targeted services. Likewise, we make it clear in our fair processing data that, unless specifically required by the service we do not process financial data. We also limit processing of information about other parties to what is relevant to that child – so for example, we may record the relationship status of the parents and the presence of siblings and other adults in a house, but probably not their employment unless there was a specific reason to.

So it's about balance?

Beyond that, where a case-file is maintained, we do try and build up a full picture of the child, reflecting the circumstances in which they live, the important figures in their lives and any other information that is relevant to us providing that child and their family with the best possible service. This is balanced with a clear Fair Processing Notice, obtaining consent at the point that sensitive personal data is first processed (we do not attempt to rely on any other Schedule 3 conditions), a no-charge policy for Subject Access Requests from service users or their representatives and what should be a transparent process of gathering and processing their data.



'Information is one of our largest assets and protection of it is one of our most important duties - we view ourselves as custodians with ethical as well as legal responsibilities to ensure it is handled and held properly'

Principle 4: Ensuring data is accurate and up-to-date

4.4

The DPA says:

'Personal data shall be accurate and, where necessary, kept up to date.'

The fourth principle is concerned with preventing prejudice to individuals as a result of incorrect or out-of-date information about them being processed.

Therefore you should:

- ✓ 1. Be able to demonstrate that your organisation takes reasonable steps to ensure the accuracy of any personal data you obtain.
- ✓ 2. Record the sources of personal information you receive.
- ✓ 3. Ensure challenges to the accuracy of personal information are given proper consideration. As a matter of best practice it is advisable to record the challenge and the response provided, particularly where the information is highly sensitive.
- ✓ 4. Consider the processes by which personal data can be updated, either by the data subject or by someone else at their request because the individual's details are out-of-date and ensure there are procedures in place to follow-up on all such requests.
- ✓ 5. Ensure adequate safeguards are in place to prevent malicious alterations of personal information by those inside and outside of the organisation.

Key questions: Who is responsible for keeping information up-to-date?

How sure can we be that the information we hold is accurate – who provided it?

How often do we check back with individuals that we still hold their correct information?

How do we ensure that we synchronise our systems so that we have correct information in every location where an individual's data is held?

FIRST FINE FOR BREACH OF RULE ON ACCURACY

In 2012 the UK regulator fined insurance and pensions giant Prudential £50,000 following errors on its database. The breach saw two separate customers with the same first name, surname and same date of birth, switched around, causing thousands of pounds from one of the individual's retirement funds to be placed in the other's. The breach happened despite a warning from one of the customers which signalled that the error was present.

Principle 5: Retaining data

4.5

The DPA says:

'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

The fifth principle is concerned with ensuring that information which is no longer in use is destroyed as soon as possible.

The DPA does not set out retention periods and you should be able to justify why you retain personal data for as long as you do by relating your retention period back to the purpose for which you collected it in the first place. Therefore you should:

- ✓ 1. Ensure personal data is deleted as soon as it becomes surplus to requirements, being mindful of how you treat parallel paper and electronic records. Do you delete both at the same time or should your policy recognise a valid reason for keeping one longer than the other?
- ✓ 2. Anonymise personal data when you no longer need to know who it relates to. Data is only personal when it relates to an identifiable, living individual. Remember that to be properly anonymised, it should be impossible for your organisation to identify the individual who it relates to.
- ✓ 3. Securely archive personal data such as case files which are no longer in use but must be kept (CVs or employment records for example).
- ✓ 4. Ensure that data subjects know what will happen to their data when they terminate their membership, ask to be removed from the fundraisers database or leave a service you provide.



Guidance from the ICO states that

"It is good practice to make it clear to people what will happen to their information when they close their account – i.e. if it will be deleted irretrievably or simply deactivated or archived.

Remember that if you do archive personal data, the rules of data protection, including subject access rights, still apply to it."

It is important to remember that deleting data is a form of processing. The data controller is responsible for protecting that personal data whilst it is being destroyed. A number of fines have been issued to data controllers who have attempted to destroy personal data but have done so in a way that increased the potential for the individuals' data to be compromised.



Key questions: Do we securely delete/ destroy personal information as soon as we have no more need for it?

Are we holding any data we no longer need?

How do we decide whether we still need our data?

Is there any data we do still need that can be anonymised or at least archived?

HITTING THE HEADLINES: FINE FOR COUNCIL WHOSE RECORDS WERE FOUND IN A SUPERMARKET CARPARK

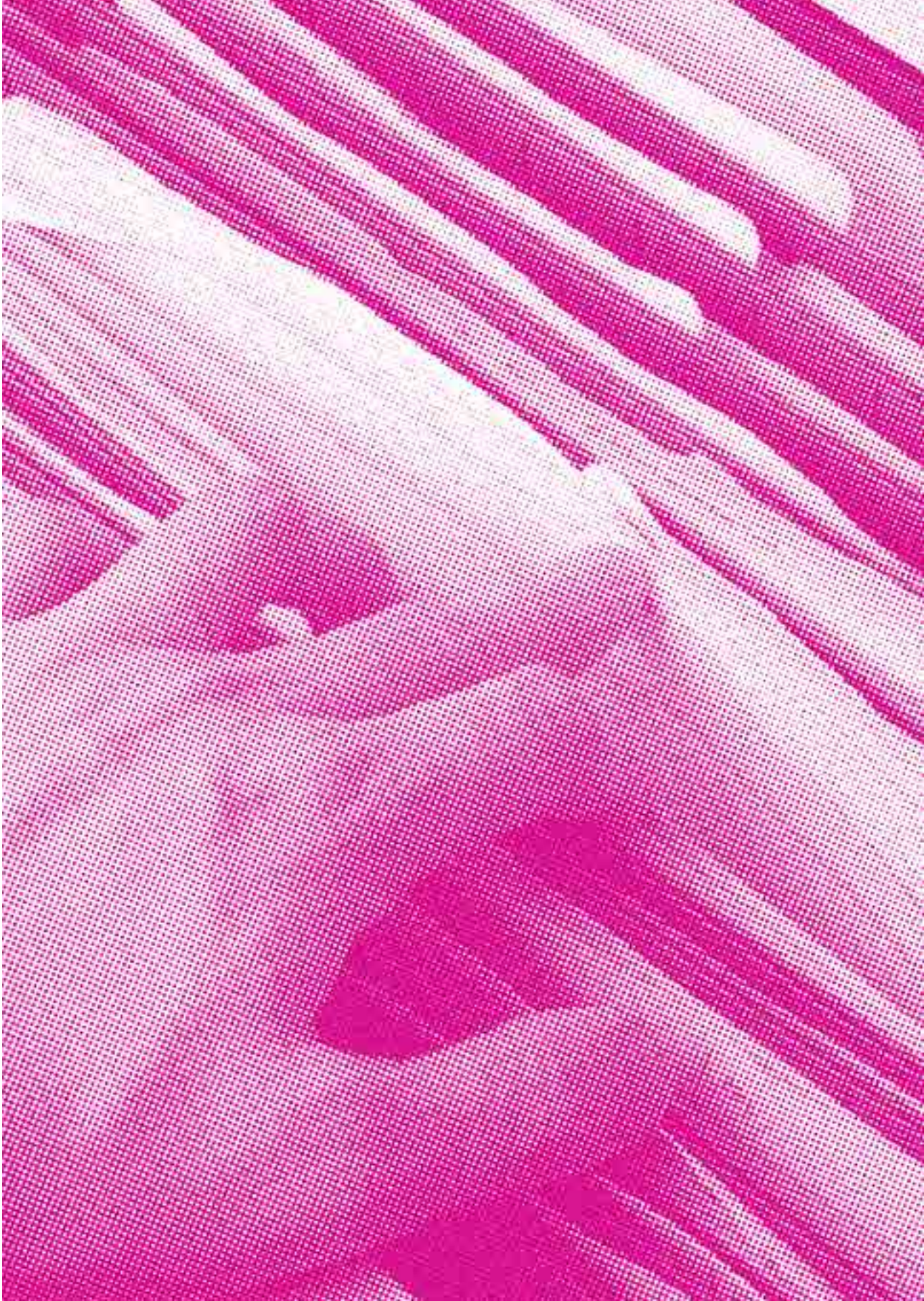
A Council whose former employees' pension records were found in an over-filled paper recycle bank in a supermarket car park has been fined £250,000 for the data breach. The council employed an outside company to digitise the records, but failed to seek appropriate guarantees on how the personal data would be kept secure.

Although this was also a breach of principle 7, it is important to bear in mind how your data will be disposed of as the data controller is responsible for the individuals' data until it has been completely destroyed.

The following table shows a range of considerations you may wish to take into account when deciding what to do with data which is no longer in general use.

	Yes	Maybe	No
Is there a minimum time you must keep it for by law?	Files that are still covered by retention periods should be archived.	Unsuccessful candidates for jobs have just 3 months to bring a claim for discrimination. In some cases an action for negligence can be brought up to 6 years after the loss was suffered and some occupational health records now have to be held for up to 40 years. Guidance from the ICO says that records should be kept according to the statutory retention periods for a claim.	The data should be deleted.
Has a third party asked you to keep it?	In certain situations someone you do business with may require you to keep records for a certain amount of time. Indemnity insurers for example will sometimes require client records to be kept for as long as it is may be possible for someone to bring a claim in negligence against you.	Review your need to keep the data and encrypt it as a minimum if you are required to keep it but don't need to use it. If you decide you have no obligation to keep it, the data should be deleted.	The data should be deleted.
Do you need it for new or different purposes?	Retain the data for as long as necessary in connection with the new purposes, but you should also notify the ICO and the individual(s) that you are processing personal data for new purposes.	You should reduce the amount of data you hold to the bare minimum, for example when a member of staff leaves, or when a job is filled – you need only keep the minimal information you will require. If for example, you wish to retain applicants data for equal opportunities monitoring you can keep a tally of the number of people applying without recording any identifiable information.	The data should be deleted.

	Yes	Maybe	No
Have you told the subject when and how you will dispose of it?	You should ensure that you treat people's data in the way that you have told them you will. If you have told people that their records will be deleted then you must delete them. It is important to be mindful of this when people ask to be deleted from your marketing database etc.	You should review the privacy notices given at the time of collecting the data in order to determine whether the subject has any expectations. If not, you should decide whether it is practicable or desirable to inform them now, if not, proceed as "no".	If the subject is unaware that their data may be kept once they leave the organisation, cease to be a member etc, you will not need to notify them that you wish to use it for statistical or research purposes if you anonymise it. If the information does not relate to an identifiable living individual it will not fall within the scope of the DPA.
Do you need to know who the information relates to?	If you need to know who the data relates to only to corroborate the information or to follow it up later you could anonymise your records using a code that does not relate to an identifiable characteristic. This will reduce the risk of accidental exposure, where for example case notes are left unattended.	If you may need to identify the subject of the data at a later date you could anonymise the record using a code that does not relate to any identifiable characteristic and restrict access to the code. Whilst this does mean the data will still fall within the scope of the DPA it reduces the risk of accidental exposure.	If you do not need to know who the information relates to but it is useful for research and producing statistics you should anonymise the information. The DPA only covers information where there is a living identifiable subject.
Can you envisage being asked for it where it would matter that you didn't have it?	You are therefore justified in keeping this data, but even when it is out of use you must still follow the principles. As a matter of best practice it is often helpful to store historical data separately and restrict access to those who need it at the time.	Personal Data should not be kept "just in case". You should at least consider anonymising the information so that it no longer constitutes personal data (only personal data must be processed according to the principles – anonymous information does not fall within its remit).	The data should be deleted or anonymised. Bear in mind that deleting is still a form of processing and so must be done in accordance with the principles. You should consider shredding to dispose of paper records and ensure no trace of the information is left in electronic format. This could include email trails etc.



Principle 6:

Rights of individuals

4.6

The DPA says:

'Personal data shall be processed in accordance with the rights of data subjects under this Act.'

The sixth principle protects six rights of individuals in relation to the processing of their personal information, of which the right to prevent processing for direct marketing and the right of access are likely to be the most significant in terms of your data protection policy.

Charities might hold information about:

- Beneficiaries and service users;
- Staff, potential or former staff and volunteers;
- Donors;
- Suppliers.

The rights under principle six are:

- a right of access to a copy of the information that you hold about them;
- a right to prevent processing for direct marketing;
- a right to object to processing that is likely to cause or is causing damage or distress;
- a right to object to decisions being taken by automated means;

Other relevant rights in the DPA are:

- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to claim compensation for damages caused by a breach of the DPA (the consequences of which are covered under enforcement and penalties on page 69).



Therefore you should:

1. Understand individuals rights for direct marketing.

Principles 1 and 2 of the DPA, that data must be processed fairly and according to specified purposes have the effect of restricting the circumstances under which you can carry out direct marketing under principle 6. According to the ICO direct marketing does not just refer to selling products or services to individuals, it includes the promotional activities of charities as well.

The effect of the law is to allow individuals not just to require organisations to stop sending them marketing materials but also to cease or not to begin processing personal data for the purposes of direct marketing. It should be noted that "marketing materials" is defined widely in the DPA so that it includes "not just the offer for sale of goods or services, but also the promotion of an organisation's aims and ideals".

This can be a tricky area for charities to negotiate, particularly where they wish to send newsletters which are not directly aimed at selling a product or service, or even making a fundraising ask but are intended to keep the recipient up-to-date. Such materials may well fall within the category of marketing materials, so you must be careful.



You should also consider whether your system is capable of allowing people to choose the information they wish to receive. There may be a number of supporters who wish to receive newsletters updating them on the progress of a project they have already donated to, who don't wish to receive further fundraising emails. If your system is unable to cope with such requests, you may risk alienating those valuable supporters. A number of online email marketing systems are available (and are free to use) that will record and filter an individuals' preferences for you, so you may wish to consider one of these systems as one method of monitoring and filtering marketing emails.



You should also consider how your preference system deals with conflicting indications. For example, if an individual has previously opted into an email newsletter and then ticks the box on an order form for 'no future marketing' will that override their newsletter choice or not?



2. Understand what to do if you receive a subject access request (SAR).

Anyone you hold data about has the right to request to see it. This includes physical data which is held as part of a 'relevant filing system' as well as electronic data. You can charge a fee of up to £10 to cover the administrative costs of dealing with their request (or £50 for certain medical records) and have up to 40 calendar days to respond. The data controller need only respond to a valid SAR, so must first decide whether a request meets the legal requirements and respond to those which do.

What constitutes a valid subject access request?

- a.** A valid subject access request must be made in writing. Electronic means such as email and fax are included within this.
- b.** You can ask subjects to fill out a subject access request form in order to help you process their request in an orderly manner, but you still have to comply with a request received in writing even if it isn't on your standard form. You might want to ask questions in order to verify their identity.
- c.** You should ensure your data protection policy nominates someone who will be responsible for dealing with subject access requests. This will usually be the data protection officer, but there may be circumstances (such as where the request comes from a former employee) that it will be appropriate from someone else, such as someone in the HR team of a larger organisation, to process the request.

You do not have to treat a subject access request as valid if it is made too soon after the same subject has made a similar or identical request. If there have been no changes it may not be appropriate or necessary to resend the data you hold.

What information must be provided?

You should provide information as it was at the time the request was received. You cannot make changes to a person's records unless they are changes you would have made anyway. Attendance at an event for example can be added to the record, or it can even be deleted altogether. The important thing is to be able to show that you have acted in the same way as you would have done were it not for the request.



More information can be found on the ICO website about:

- subject access requests
- employee rights and employment references

- You should provide a copy of all the Personal Data you hold about the subject unless:
- It is not possible to do so; or
 - It would involve disproportionate effort; or
 - The data subject has agreed otherwise; or
 - Another exemption under the DPA applies.

You should be wary of disclosing information about another individual (third party) unless the third party has consented to the disclosure or it is reasonable to disclose it without consent. This is often one of the trickiest areas to deal with in relation to SARs and you may sometimes need to take professional advice because there can be serious consequences for disclosing third party materials which should have been kept confidential.

3.Ensure you comply with the marketing requirements under the Privacy and Electronic Communications Regulations

About the Privacy and Electronic Communications Regulations

The Privacy and Electronic Communications Regulations (PECR) were introduced in 2003 and updated in 2011 by European law and apply further restrictions to the DPA on emails, fax, texts and telephone communications. The PECRs distinguish between individual subscribers and corporate subscribers with the effect that there are fewer restrictions on sending marketing materials to corporate subscribers. But it should also be remembered that in some cases a 'work email address' might constitute personal data and therefore the individual could exercise their rights under the DPA. In any event, good practice should dictate that you would not wish to send promotional materials to people who clearly don't wish to receive them.

Where the recipient is joebloggs@companyx.com you do not need prior consent to send them unsolicited marketing. However it is best practice to send marketing to them as if they were private individuals.

What about charities?

If your mailing list or fundraising database includes work email addresses of people who work for charities you should be careful. Both the DPA and PECR give some indication on what constitutes a corporate subscriber, but they essentially hinge on whether or not the company has been incorporated.



More information can be found on the ICO website about:

- charities and marketing

The majority of larger charities are incorporated, but some small ones won't be. This means that, if there is uncertainty you should, as a matter of best practice, treat joebloggs@charityx.org as an individual subscriber. Following on from this logic, in most cases, you must have prior consent to send them direct marketing.

What is meant by prior consent?

Prior consent for the purposes of the PECR can be attained by either opting-in to receive communications, or by opting-out. The matrix below will help you to decide which method is most appropriate for you, but is important to remember that, although there is vast amount of guidance and opinion as to which method is most suitable, the most important consideration should be to ensure the data subject knows what they are signing up to.

Desk Top Guide to the marketing requirements of the Privacy and Electronic Communications Regulations 2003 (PECR)

Regulation	Individual subscribers joebloggs@personalemail.com joebloggs@unincorporated.org	Corporate subscribers joebloggs@company.com joebloggs@incorporated.org
Automated Calls	Do not make unsolicited automated marketing telephone calls without prior consent	Do not make unsolicited automated marketing telephone calls without prior consent
Faxes	Do not send unsolicited marketing faxes to individual subscribers without prior consent	Do not send unsolicited marketing faxes to numbers which are registered with the FPS
'Live' Telephone calls	Do not make unsolicited marketing telephone calls to subscribers who are either : - Registered with the TPS or CTPS or Have previously asked the company not to call them	Do not make unsolicited marketing telephone calls to subscribers who are either : - Registered with the CTPS or TPS or Have previously asked the company not to call them

- Key questions:** Do we have permission to contact people for marketing purposes?
- Would we know what to do if a member of staff, volunteer or service user asked for a copy of the information we hold about them?
- Do we have a nominated data protection officer, or someone who will be responsible for responding to SARs?
- Have staff received sufficient training to recognise an SAR and forward to the appropriate person if we were to received one?
- Do we know what exemptions may be relied on which would allow or require us to withhold records from disclosure?

Regulation	Individual subscribers joebloggs@personalemail.com joebloggs@unincorporated.org	Corporate subscribers joebloggs@company.com joebloggs@incorporated.org
Electronic Mail – Text messages, e-mails etc	<p>Do not send unsolicited marketing material by electronic mail to individual subscribers without prior consent.</p> <p>Only exception to this rule- the 'soft opt in'</p> <p>Only applies where a company can meet all three criteria</p> <p>1. The company have obtained the contact details for the recipient in the course of a sale, or the negotiations for the sale, of a product or service to that recipient.</p> <p>2. The direct marketing material they are sending is only about their own similar products and services.</p> <p>3. the recipient was given a simple means of opting out at time their details were initially collected and is given an opt out opportunity at time of each subsequent communication.</p>	<p>No prior consent requirement for sending electronic mail marketing to corporate subscribers.</p> <p>However do need to identify yourselves and provide valid address for opt outs in communications.</p>

The ICO provides examples of opt-in/opt-out statements, all of which are compliant with the sixth principle and the PECR because they are clear and demonstrate that the individual wishes to receive marketing information.

When working with inherited databases, or those which may contain contacts' details obtained before the DPA and PECR came into force it is important to ensure that your contacts are aware that they may receive marketing messages from you. For more information on informing inherited or prior contacts how you will be communicating with them, see the Conciliation Resources case study on page 25.

'Staff training based on anecdotes, analogies and 'what if' scenarios as well as practical advice was very successful in closing the gap between abstract awareness of the importance of data protection and knowledge of how to apply good practice to everyday tasks'



Principle 7: Information security

4.7

The DPA says:



More information can be found on the ICO website about:

- security measures

Key questions: Are our physical records, IT equipment and building secure?
Do we know who is in the building i.e. visitors, volunteers, cleaners, service users?
Is the website secure?
Is data encrypted in transit, including when stored on portable devices such as laptops or blackberries?
Are systems designed to restrict access to those who need to know, and are these access controls enforced and monitored?
Do we have a policy for home and remote working?
Do staff know what information can be taken in and out of our secure environment?
Have staff been trained in their responsibilities under the DPA?
Do staff and volunteers know how to respond if asked for personal information e.g. not to disclose personal information, or how to recognise a subject access request?

‘Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.’

The seventh principle is concerned with ensuring the security of personal data and requires data controllers to establish measures which will prevent harm to the data subject as a result of their information falling into the wrong hands. This is often likely to occur where personal data is in transit or has been taken “off-site” e.g. for home working. The majority of monetary penalties have been imposed for “lost” data.

You should ensure that IT and email systems are secure and that staff are trained in data protection policies. As a minimum you should:

1. Know who is in the building i.e. visitors, volunteers, cleaners, service users and ensure that physical records, IT equipment and building secure.
2. Establish password procedures such as automatically expiring passwords.
3. Encrypt data when it is in transit, including on portable devices.
4. Monitor security logs showing failed attempts to log-in to your network.
5. Ensure ex-staff user accounts are disabled and passwords are changed for externally accessible systems.
6. Have a policy for home and remote working.
7. Ensure staff been trained in their responsibilities under the DPA.

Case Study

The Nuffield Trust: ensuring the security of personal data

During our Finance Committee meeting in the spring of 2012, whilst reviewing our risk register, one of our Trustees asked the question “are we really doing all we should be to mitigate the risk of data loss?” – This prompted us to review the security surrounding all of our data, not just the data we buy in for research purposes

What kinds of personal data does the Nuffield Trust process?

The Nuffield Trust currently holds two main types of personal data, which can be broadly categorised as follows:

- a. Staff and contractors details, in many cases including full names, address details and banks details; and
- b. Pseudonomised Research data, currently mainly HES Data (Hospital Episodes Statistics) from the NHS Information Centre.

Why is data protection important to the Nuffield Trust?

We have to take our data security very seriously. As a registered Data Controller with the ICO there would be serious implications to us as an organisation, and our ability to perform the detailed research analysis that forms a core part of our charitable work, if we were to lose eligibility for registration as some of our contracts stipulate it as a necessity.

Ensuring that we take every step possible to create a secure environment for all of our data is an extremely high priority. Over the past 2 years we’ve implemented some drastic changes to our structures and are constantly keeping touch with developments, mainly in IT, to ensure that we’re up-to-date with the economically viable options to suit our requirements.

How did you demonstrate this to the board?

The project started out by reviewing the existing policies and ensuring they were being adhered to. As the finance manager, I took the lead on the project and worked with the Head of Research and IT Support Officer to produce a detailed report for the Finance Committee. Producing the report resulted in us doing a full review of our systems and security measures, particularly focused towards IT risk, then summarising the policies in a manner suitable for presentation to the Board.

Following the review and production of the report, we were able to conclude that we are taking suitable measures.

How do you protect staff details?

All personal data for staff (contractors and directly employed staff) is kept within the Finance and Administration department with access restricted to 4 individuals.

- a. Physical documents are kept in locked cabinets and treated as strictly confidential. Access is not given to anyone outside of HR except the Finance Manager for payroll purposes.
- b. Electronic copies of the above documents are held in a secure folder with restricted access on the company server.
- c. Payroll details are stored on a local workstation (protected by our strict password protocol) accessible only by the Finance Manager. Regular backups of the data are taken and stored in a secure file on the company server in a folder.
- d. Contracted staff details are stored within the accounts software and are accessible by only 3 members of staff.
- e. Bank details are stored on the secure online banking portal, accessible only by authorised online bank users.

What other types of data do you have to protect?

We currently protect around 12tb of research data with our Research Governance Framework:

- a. All research data is pseudonomised, making it impossible to identify any individuals.
- b. Research data is stored on a separate, dedicated server which is only accessible to members of the Research Group with written authorisation from the Head of Research.
- c. Authorised users are required to log in using a second and unique set of log in details (separate to their usual IT login).

What technical measures do you have in place?

Since a department restructure in August 2010 and the employment of a dedicated IT Officer, all practices around our general IT security have been improved and strengthened. Having a dedicated resource has allowed us to review historic practices and identify possible shortfalls in the measures in place; we have been in a position to ensure that our procedures conform to best practice and meet the particular requirements of the Trust.

Every individual working at the Trust premises has their own dedicated workstation protected by our password protocol and user profiles cannot be accessed without a password. Individual workstations have limited storage, and the storage of any files locally is actively discouraged: all electronic files are required to be stored on our company file server (company drive) using the established folder structure. The Trust imposes complex folder access authorisations and the company drive has secure storage areas for all Network Members, in addition to the team and project specific secure areas.

- a. The server itself is only accessible to our IT officer and IT Support Contractor.
- b. The server, network and local workstations are protected against viruses and malware using industry best practice standard software.
- c. USB Storage devices are only permitted under certain circumstances as they can be a route to introduce malicious files from external sources.
- d. Entire data backups are taken weekly and sent to a secure off-site location.
- e. The data within the backup is protected by 256bit encryption at hardware level using "12 digit +" randomly generated passcodes.
- f. Daily backups are kept on site stored in fire and bomb proof containers.

How do you mitigate against the risks of remote working?

As a part of our IT restructuring in 2010, it was concluded that the Trust required a secure and reliable remote working environment. A VPN (Virtual Private Network) was inherited, but this proved to be unreliable and did not meet the necessary security requirements. A Citrix working environment protected by RSA Secure Access was

decided upon and implemented. Access to the Citrix environment is given to selected members of employed staff only and must be authorised by a member of SMT.

- a. The RSA Secure access requires a "2 Factor authentication, plus 1" – Using a combined user known passcode and algorithm automatically generated passcode using RSA, then user set password (following the existing password protocol).
- b. RSA fobs (the source of the automatically generated part of the access passcode) and Citrix access can be disabled remotely by the IT Officer.
- c. Citrix environment is monitored remotely and notifications of successful logins are sent to the IT Officer.
- d. Citrix is a dedicated and secured environment and data cannot be copied through the network to a local workstation (for example, an employee's own computer).

What about laptops?

The Trust has a pool of laptops for staff use, administered by our IT Officer. Company Laptops are set to default with no network access allowed (disabled at user level).

- a. No company file server access is allowed on company laptops (except through the Citrix environment).
- b. Pool laptops are cleared down after use by the IT Officer.
- c. A register is kept of who has borrowed laptops.

What about mobile devices?

The Trust mitigates the risk of losing data stored on mobile devices by minimising exposure; blackberries are issued only to employees deemed to require one.

- a. Blackberries have a passcode protocol and can be remotely cleared at server level, wiping all data on the device and rendering it unusable.
- b. Blackberries are set up to only store emails for 30 days, anything older is automatically deleted from the devices memory.

What steps do you take to secure your networks?

Access to the internal networks at the Trust is governed by our username and password protocol, in addition to which firewall and internet protection is provided at 2 points: we have an internal hardware based firewall, plus a cloud based gateway.

- a. Both provide a customisable solution to restrict traffic to inappropriate or potentially dangerous internet resources and incoming traffic from unrecognised or dangerous sources.
- b. Restrictions can be set through generalisation (adult nature) or using the customisable platform identifying specific web addresses.
- c. The firewalls also act to restrict downloading suspicious or dangerous files.

How do you know your networks are secure?

The Trust has recently taken steps to have the integrity of our IT security tested by an outsourced contractor. An External Network Vulnerability test (Penetration Test) was carried out. The objectives being: (1) to test the existing security and (2) identify any potential causes for concern in a controlled manner using a trusted and certified contractor. The method was to test the access gateways to our internal data through available external sources, principally by Website and IP attack – in layman's terms; to hack into our network through the internet.

Could a visitor connect to your networks?

There are 2 internal Wireless network zones. The "Visitor" zone is accessible by members of the public by way of a username and password available from our IT Officer. This public zone is a demilitarised zone and is completely separate from all of our company IT resources; it shares access to the internet only (by way of a shared gateway) and access to our file server is not possible..

- a. All Wi-Fi zones are protected by WPA2 encryption.
- b. There are no wired network points currently live but unused so an unauthorised individual would not be able to connect their own hardware to the system.

What organisational measures do you have in place?

The Trust has a data handling and confidentiality agreement which stipulates that all data is the property of the Trust; staff are not to intentionally share data with unauthorised persons and anyone found to be breaking the terms of the agreement could face HR disciplinary action.

- a. Everyone working within the Trust (whether an employee or not) signs the data handling and confidentiality agreement as part of their HR induction.
- b. Hard copies are kept in HR Files.
- c. Employment contracts state that the document must be signed prior to commencing employment.
- d. Contractors working on data or company drive are required to sign prior to any work commencing.
- e. Local workstations are protected by the company password protocol Staff are frequently reminded of the terms of the protocol, which include disciplinary action.
- f. Passwords should be no fewer than 8 characters, they should not contain a word in English or a foreign language or a name and should contain at least 3 of the following: a numeric, upper case, lower case, punctuation and symbols.
- g. Users are required to ensure that sensitive data cannot be viewed by other persons nearby.
- h. Workstations must be locked when a user vacates his or her desk.
- i. The office is accessible using an unidentifiable electronic key fob and all visitors are required to be granted access by an internal member of staff.
- j. Every evening, a contractor secures the building and activates the intruder alarm.

Principle 8:

Transfer of data abroad (outside the EEA)

4.8

The DPA says:

'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.'

The eighth principle is concerned with ensuring personal data is kept safe when transferred abroad. The DPA therefore prohibits the transfer of personal data outside of the EEA unless it is possible to ensure it will be adequately protected.

The EEA: The European Economic Area comprises all countries of the EU and in addition, non-EU countries Iceland, Liechtenstein and Norway. Transfer of personal data to countries in the EEA is permitted by the DPA. It is important to remember though that all transfers of personal data (inside the EEA or otherwise) must still be conducted in a way that is compatible with the other seven principles.

STEPS. Guidance from the Information Commissioner recommends the following approach:

1. Consider whether there will be a transfer of personal data to a third country (one which is not in the EEA). If so;
2. Consider whether the third country ensures that an adequate level of protection will be given to the data, either because the EU has deemed it to be adequate or if not by conducting your own assessment of adequacy if a decision has not already been made by the EC on that country. If not:

3. Consider whether the parties have adequate safeguards or can put them in place either by entering into model clauses approved by the EC or establishing binding corporate rules. If not;

4. Consider whether any other alternatives permitting the transfer, such as consent of the data subject, apply.

For charities that are less able to dedicate resources to legal research or drafting model clauses, the order in which you approach your options is likely to be different to the one listed above. The following order is based on the risk of harm to the data subject arising as a result of the transfer of their data, and the cost implications of the various options available.

1. Consent.

The first option you should consider is consent. This is usually the most appropriate course of action for personal information relating to employees or volunteers, where it is easy to communicate with and obtain consent from the data subjects are easily communicable. Charities with overseas operations frequently find themselves having to send details of those employees to the territories in which they will be working. The law does not state that you automatically have the consent of an individual applying for a position abroad to transfer their personal information.

However, the chance of such an individual objecting to the transfer and the ICO enforcement action being pursued against you is likely to be very low in reality. Nonetheless it will help ensure your organisation is legally compliant if the data protection statement on any application or registration form that the individuals fill in should state that personal details may need to be transferred outside of the EEA and that by submitting the form they consent to this transfer which is necessary for the role.

2. Approved countries.

There is a list of countries whose laws on data protection have been assessed by the EU and found to serve similar protection purposes, this is known as a community finding of adequacy. If a country appears within this list, personal data can be transferred to that country without breaching the eighth principle. At the close of 2012 the following countries had been recognised by the Commission as providing an adequate level of protection (either through their own law, or entering into international agreements).

- Andorra
- Argentina
- Australia
- Canada (in some circumstances)
- Faeroe Islands
- Guernsey
- Isle of Man
- Jersey
- State of Israel
- Switzerland

The Commission has also recognised the following US institutions as providing adequate protection:

- a. United States' Bureau of Customs and Border Protection in respect of the transfer of Air passenger name records.
- b. Organisations which have self-certified their compliance with the US Department of Commerce's Safe Harbor Privacy Principles.

Key questions: Do we send personal data outside of the EEA?
 If so, does it go to one of the countries already approved by the EC?
 If not, do we have consent to transfer the data?
 Can we use the model clauses to transfer the data?
 If the recipient is in the US, have they signed up to the Safe Harbour rules?

The US – EU Safe Harbour List details organisations that have committed themselves to comply with the Safe Harbour Framework and will therefore provide adequate protection for personal data from the EU. If an organisation appears on the list, you can be satisfied that they will protect the personal data you send in a way which is compatible with EU law. In the event of a breach, you will be able to demonstrate, by reference to the list that you were assured of adequate protection when you made the transfer and should not be at risk of enforcement action from the ICO. You should be aware that non-profits cannot sign up to the Safe Harbour Agreement as they are not regulated by the Department of Commerce.

3. Assessment of adequacy.

An assessment of adequacy can also be made by the data controller itself, although care should be adopted in taking this approach. In general, we recommend that professional advice should be sought before proceeding with an assessment. The case study below from Charity X explains their experience of transferring data abroad.

4. Legal processes. There are a couple of other options available, when drafting contracts with data processes outside of the EEA but these were designed with the large business in mind. They are likely to require significant input from lawyers at a considerable cost, but are options nonetheless.

Case Study

Charity X: Transfer of data abroad

NOTE: This example refers to very specific circumstances. In general it is not recommended that charities undertake their own assessment of adequacy.

Charity X is a charity which operates internationally. Charity X has a large number of individual supporters which it retains in a supporter database. It doesn't hold any sensitive data about supporters, but deals in very large volumes of supporter data, and uses its database to make contact with supporters through various communications channels, both to fundraise, and to support its campaigning efforts.

Why is data protection important to Charity X?

Charity X takes its responsibilities for data protection very seriously. This is both from a need to meet its statutory responsibilities, and to fulfil the trust its supporters place in it. This trust is an essential part of the relationship between Charity X and its supporters.

What did Charity X wish to achieve with its data, and why?

Charity X is in the process of working with associated charities in several other countries to raise funds, and deliver their work. Part of that joint effort involves identifying where supporters are located, and which charity is best placed to deal with those supporters.

In order to do that Charity X wanted to provide access to one of these associated charities to allow them to identify supporters in their country whom may be better served in that country, rather than by Charity X directly.



More information can be found on the ICO website about:

- sending data overseas

Working together with its international partner in the USA, Charity X identified that there was a need to transfer information about some individual supporters to the partner. Creating a separate database was considered undesirable, as it would significantly increase the risk of duplicate records or other forms of data corruption. Therefore Charity X decided to allow its partner to have access to its supporter database over a VPN. This would create a transfer of personal data outside of the EEA.

What did Charity X do about it?

Having determined that there was a need to transfer personal data outside of the EEA, Charity X set up an internal team to consider how to provide this transfer in a manner which is compliant with the DPA.

This team reviewed all of the available options for compliance with Principle 8. Many of these were disregarded early in the process as not being suitable for a charity of its scale or particular needs.

- a. It was considered impractical to contact all supporters and get their consent to transfer the data, and there was no reasonable implicit consent to transfer their data.
- b. A binding corporate rule appeared to be an onerous option, and possibly unsuitable for two independent charities which are closely associated, but have no formal control over each other.
- c. The partner charity is based in the USA, which is not approved as a providing adequate protection by the European Commission.
- d. The partner charity was not able to make use of the Safe Harbour accord, as it is registered as a non-profit in the USA.
- e. The use of contracts with model clauses was an available option, but would have involved legal costs, and would do nothing to reduce any of the real risks of losing data.

Having reviewed all of these options, Charity X decided to undertake an assessment of adequacy with the intention of allowing it to provide access to its supporter database in a way which was compliant with Principle 8.

Charity X came to the following conclusions on the general adequacy criteria.

General adequacy criteria	
The nature of the personal data	None of the data could be regarded as sensitive, either as the term is used in the Data Protection Act, or in any more general sense.
The purposes for which the data will be processed	<p>The data would be processed in order to better communicate with supporters, and provide them with information which is most suited for their needs.</p> <p>In its fundraising and campaigning uses, it would be employed to further Charity X's objectives. The very objectives which supporters had chosen to support in providing their information.</p> <p>Access to the database would be very limited. Contact with supporters using information in the database would be subject to strict controls agreed between Charity X and their partner.</p>
The period during which the data will be processed	The intention was to provide on-going access. However it was expected that the access would only be needed intermittently.
The country the data was collected in	<p>The data was mainly collected in Britain, with a relatively small proportion from other countries. Of those other countries, the largest number of supporters were themselves based in the USA.</p> <p>No country-specific expectations for supporters were identified.</p>
The final country you are transferring data to	<p>The data was to be transferred to the USA, which shares significant elements of common culture with Britain. These considerations include a shared language, tradition of common law, and similar expectations of personal privacy.</p> <p>There would be no transfer onwards to any other country.</p>
Security measures taken in the country you are transferring to	<p>This was deemed to be the most substantial part of the assessment.</p> <p>The team, led by Charity X's Internal Audit function, undertook a review of the IT security measures in place at the partner, as well as the capacity of their staff and systems to safeguard data.</p> <p>This review found the systems in place at the partner to be largely adequate. It made a number of recommendations on systems improvements with the intention of providing additional assurance over the security of data transferred.</p>

What did this mean for Charity X's work?

Charity X has been able to coordinate its fundraising and campaigning efforts with its partner better. It is anticipated that this will lead to improved future income, and scope to influence in pursuit of its objectives.

The exercise itself provided an opportunity to review and improve the security of personal data, and provided additional assurance over this key responsibility.

Do you have any top tips for others conducting their own assessments?

- a. In assessing general adequacy, it's important to keep the potential harm which data subjects could face if their data was misused. All the first seven principles are applicable to the assessment.
- b. You might be undertaking the assessment to meet your obligations under the DPA, but consider the reputational damage that your organisation could face if it fails to appropriately safeguard data. This could provide an opportunity to review real-world controls.
- c. Most of the general adequacy criteria help set the context for what data you're going to transfer, and why. The last criterion gets to the meat of measures that could actually protect data, safeguard your reputation, and treat data subjects (whether they are supporter, staff, volunteers, or others) fairly. This is where you should focus the greater part of your attention.
- d. If you're dealing with a third-party, you can make the legitimate claim that you have a legal obligation to do this, and that you have to do it. However, it can also be sold as an opportunity for them to consider and improve their own controls.



'The thing that worked for us was getting senior management buy-in'

Other considerations

5.1

Credit cards

Credit card payments are an accepted and essential part of how most charities do business. Standards such as the PCI DSS exist to ensure that details are held and processed securely but these can be tricky to negotiate and fit in with your information security.

5.2

Enforcement & penalties

It is the role of the Information Commissioner to ensure that all organisations responsible for processing data comply with the DPA and the PECRs. In the event of a breach, or possibility of one a number of options are available to the ICO either to enforce compliance or penalise those who are not complying. These include:

Enforcement measures are taken by the Information Commissioner to encourage a data controller to comply. They are not penalties in themselves but failure to adhere to them could result in one.

Consensual audit: Although not strictly a penalty for a breach that has already occurred, the ICO may from time to time offer a consensual audit. This is sometimes offered as a response to complaints or where the ICO believes a particular body faces a higher risk of a breach. These audits are carried out with permission of the data controller, and executive summaries of each are published on the ICO's website and available to the public. A full report will be written for the organisation detailing steps they can take to ensure compliance and these will often be



More information on PCI standards is available here:
<https://www.pcisecuritystandards.org/>

followed up on. Consensual audits can be requested, but the ICO will allocate its resources to the highest-risk data controllers. To identify high-risk data controllers and sectors the ICO uses a number of sources, including:

- business intelligence such as news items;
- data controllers' annual statements on control and other publicly available information;
- the number and nature of complaints received by the Information Commissioner; and
- other relevant information.

a. Information notices: Can be issued to the data controller, asking them to provide specific information within a specified time to enable the Commissioner to decide whether the principles are being complied with.

b. Enforcement notices: May be issued by the Commissioner where there has been a breach in order to ensure future compliance by the Data Controller. An enforcement notice will detail the necessary steps to be taken, and failure to comply is an offence in itself.

c. Monetary penalties: The ICO has had the power to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010, and serious breaches of the Privacy and Electronic Communications Regulations. A monetary penalty will only be appropriate in the most serious situations. When deciding the amount of a monetary penalty, the Commissioner not only takes into account the seriousness of the breach but also other factors including the size, financial and other resources of a data controller. It is not the purpose of a monetary penalty to impose undue financial hardship.



More information on penalties is available on the ICO website:
<http://ico.org.uk/enforcement/fines>

5.3

BYOD



Bring your own device, is a trend identified by ENISA as one amongst its top risks and opportunities. In a sector where resources are scarce, having staff and volunteers work from their own devices presents a great deal of opportunity for cost savings as well as for flexible working arrangements. No opportunity is present without risks. The key risks you should consider can be summarised as:

- a. It may be difficult to enforce a data protection policy on a users' own device.
- b. The risk for potential unauthorised sharing or hacking of a users' own device is greater as it can be difficult to ensure that adequate software and protections are installed on a user's own device.
- c. It can be difficult to determine who data belongs to when created or stored on a user's own device.
- d. Mobile devices with access to network drives are at greater risk of loss or theft whilst in transport.
- e. Users whose devices have already been compromised (either deliberately ie. to "jailbreak" or maliciously) are more susceptible to further attack.

5.4

The cloud



Cloud computing brings opportunities for cost savings and creates potential for flexible working arrangements. However, cloud computing is not a standard outsourcing process; it should be seen as a service and decisions surrounding its implementation made accordingly.

- a. It is the duty of the buyer to ensure that the service they purchase complies with the law. This includes the data protection principles. Most cloud service providers will use standard term contracts, so it is for you to ensure that these terms work for your needs. Many providers who are incorporated in the USA will be participants in the Safe Harbour programme, but you will need to read their entry in the Safe Harbour register to see whether it recognises their status as a data processor (not just as a data controller for their own purposes) as most don't.
- b. In many cases the company selling you the service will not be the same as the company providing you with the physical capabilities. This means that accreditations such as ISO27001 may have been awarded to the service you are buying but not to the company who maintain your physical servers etc.

- c. Using cloud computing can increase your risk of an attack from a malicious insider as an unintended consequence of an attack on another party with whom you share network.

Collaboration

Increasingly organisations are working together to make cost savings or working together on projects to serve mutual interests. The relationship needs to be analysed to determine who the controller is and what protections need to be put in place.

Training for your staff



Training staff is really important in terms of ensuring that data protection is properly implemented across your charity.

More information is available on the ICO website about:
- training your staff, including the 'Think Privacy Toolkit'

Employment



As an employer, charities are responsible for ensuring their employees' personal details are respected and properly protected.

More information is available on the ICO website about:
- employment, including a 'Quick guide to the employment practices code'

Outsourcing



Some charities outsource the processing of personal information eg payroll function or customer mailings. Data protection also applies in these instances.

More information is available on the ICO website about:
- outsourcing, including 'Outsourcing: A guide for small and medium sized businesses'

The end of the road

Many charities are closing down due to increasing financial pressure. Data protection should remain on the agenda when they wind down or merge with another organisation.

OTHER USEFUL RESOURCES:

Data Protection for Voluntary Organisations, Paul Ticher, 3rd edition 2009.

Data protection policy: <http://www.ncvo-vol.org.uk/advice-support/ict/managing-ict/data-protection-policy>

Charities and Marketing, ICO: http://www.ico.org.uk/for_organisations/sector_guides/~media/documents/library/Data_Protection/Practical_application/CHARITIES_AND_MARKETING_12_06.ashx

Data Protection for Fundraisers, L Simanowitz and M O'Reilly, <http://www.spmfundessentials.org/titles/data-protection-for-fundraisers>.

Case Study

Glyndebourne: credit card security

Glyndebourne opera prides itself on a passion for artistic excellence. This commitment to quality has earned Glyndebourne a loyal audience following enabling it to preserve artistic freedom through financial independence; although our tour and educational work receive Arts Council support, the Festival receives no public subsidy. It is essential that the company protects this special relationship with our audience; this includes being certain that their personal information is managed with the care and respect that they deserve.

As with many charities, Glyndebourne manages several types of personal information including customer data and transactions, staff information and credit card transactions via the shop, membership, box office and web. All aspects of data protection are carefully considered and controlled, but none more so than the management of credit card data where there is a dual risk because of the internationally-increasing incidence of credit card fraud.

Why is data protection important to Glyndebourne?

One of Glyndebourne's most valuable assets is its reputation/brand and anything that contravenes the Data Protection Act, in particular to do with credit card fraud or misuse of financial data, would have a catastrophic effect on the company's reputation. Glyndebourne is a membership organisation that relies on repeat business from a select group of individuals who trust us – this trust is inherent to our success and as such, protecting privacy and financial data is integral to maintaining the business. Glyndebourne processes around 50,000 card transactions each year – that's 50,000 opportunities to lose that valuable trust from members, each of which would quickly have an impact on business

How do you keep credit card details secure?

Working with specialist external advisors, Glyndebourne conducted an internal audit of its credit card security arrangements, assessed against payment card industry standards (PCI DSS). At first appearance the requirements of the standards seemed impossibly onerous but by using the PCI Security Standards Council Prioritised Approach it was relatively straightforward to understand what steps were necessary. Glyndebourne has used this approach both to assess its level of PCI compliance and to develop a clear plan for the future.

Specific actions addressing the Prioritised Approach milestones include:

1. Ensuring that sensitive authentication data is removed from media; one example of this is members' ticket requests. Glyndebourne members are able to purchase tickets for operas in advance of the general public during a priority booking period, the requests entering a ballot; this necessitates holding payment information during a short period between the opening and closing of the priority booking period. Once tickets have been allocated it is no longer necessary to keep payment information, but the request forms do have to be retained. The booking forms were redesigned so that card information is on one corner, which is cut off and shredded – a simple, effective and extremely 'low-tech' solution.
2. Where low-volume card transactions are processed on a card terminal the card number is redacted; use of indelible black pen makes card information unreadable and the merchant copies of transaction slips can be safely stored.
2. External and internal access to card data has been limited by the configuration of computer network architecture, including regular network vulnerability scans. Standards that describe how networks with different levels of trust and access requirements are segregated have been established.
3. Glyndebourne has no in-house software development but aims to ensure that all applications processing cards have been configured securely by developing written configuration standards that must be followed, particularly in the area of servers that support applications that process credit card data.
4. User access to systems storing, processing or transmitting card data is monitored and controlled appropriately by use of regularly reviewed audit logs and by using automatic alerts for unusual activity.

5. Stored card data is carefully protected, primarily by encryption wherever such data is held electronically. Access to areas of the company where card data is processed is limited by physical means such as number pads on doors or swipe card access locks. In the Box Office, where the highest volume of card data is processed, staff keep handbags, mobile phones and other personal items in lockers and not at their desks to protect them from any possibility of breaching data security, inadvertently or otherwise. All visitors are required to wear badges to distinguish them from staff.

6. The policies and procedures addressing the protection of card data have been documented so that they can be rigorously followed. New staff who will be processing card data, in addition to having successfully completed an enhanced pre-employment reference check, have to read the relevant departmental data protection policy and sign a copy to confirm that they have understood it.

7. A steering committee has been established to oversee the progress towards full PCI compliance. This group is responsible for communication of card data protection requirements within the company, and responsible for keeping stakeholders (e.g. the bank) up to date with progress.

How did you find the process of reviewing your security?

Although the task of ensuring best practice in protecting credit card data and keeping it secure was initially rather daunting, many of the actions have been easily and inexpensively achieved. The key issues for Glyndebourne were motivating both management and staff to understand the importance of good data protection practices, and making the data protection policy relevant to their particular area of work.

What is the most important thing you've learned?

Anyone is entitled to challenge an organisation's approach to their data – and they do! There is nothing better for customer relations than being able to demonstrate a robust approach to this.



Data protection checklist

6.1	
1. Handling data fairly and lawfully	<ul style="list-style-type: none"> a. Do we know who our data subjects are? Eg. donors, staff, volunteers, service users, suppliers? b. Do we really need the information we collect about this group of data subjects or an individual? c. Do we know what we're going to use it for? d. Have we met one of the schedule 2 conditions? (see page 19) e. Do we process sensitive personal data? If so, have we met one of the schedule 3 conditions? (see page 19)
2. Obtaining and processing data for specified and lawful purposes only	<ul style="list-style-type: none"> a. Have we told individuals how their information will be used? b. Have we notified the Information Commissioner of the purposes for which we process personal data? c. Is our notification up-to-date? d. Are we clear internally what we have told people, so we know what purposes we can now use the information for? e. Do we have/ want to have staff details on our website? If so, have we consulted with them? f. Do we use CCTV? If so, are we displaying notices informing people that we are collecting information about them and are the cameras placed so as not to invade privacy?
3. Ensuring data is adequate, relevant and not excessive	<ul style="list-style-type: none"> a. Is this information relevant to the way we process it? b. Do we really need to have this information? c. Do we have enough information to make the decisions we do?

4. Ensuring data is accurate and up to date	<ul style="list-style-type: none"> a. Who is responsible for keeping information up-to-date? b. How sure can we be that the information we hold is accurate – who provided it? c. How often do we check back with individuals that we still hold their correct information? d. How do we ensure that we synchronise our systems so that we have correct information in every location where an individual's data is held?
5. Retaining personal data	<ul style="list-style-type: none"> a. Do we securely delete/ destroy personal information as soon as we have no more need for it? b. Are we holding any data we no longer need? c. How do we decide whether we still need our data? d. Is there any data we do still need that can be anonymised or at least archived?
6. Knowing the rights of individuals	<ul style="list-style-type: none"> a. Do we have permission to contact people for marketing purposes? b. Would we know what to do if a member of staff, volunteer or service user asked for a copy of the information we hold about them? c. Do we have a nominated data protection officer, or someone who will be responsible for responding to subject access requests (SARs)? d. Have staff received sufficient training to recognise an SAR and forward to the appropriate person if we were to received one? e. Do we know what exemptions may be relied on which would allow or require us to withhold records from disclosure?

7. Ensuring the security of personal data	<p>a. Are our physical records, IT equipment and building secure?</p> <p>b. Do we know who is in the building i.e. visitors, volunteers, cleaners, service users?</p> <p>c. Is the website secure?</p> <p>d. Is data encrypted in transit, including when stored on portable devices such as laptops or blackberries?</p> <p>e. Are systems designed to restrict access to those who need to know, and are these access controls enforced and monitored?</p> <p>f. Do we have a policy for home and remote working?</p> <p>g. Do staff know what information can be taken in and out of our secure environment?</p> <p>h. Have staff been trained in their responsibilities under the DPA?</p> <p>i. Do staff and volunteers know how to respond if asked for personal information e.g. not to disclose personal information, or how to recognise a subject access request?</p>
8. Transfer of data abroad	<p>a. Do we send personal data outside of the EEA?</p> <p>b. If so, does it go to one of the countries already approved by the EC?</p> <p>c. If not, do we have consent to transfer the data?</p> <p>d. Can we use the model clauses to transfer the data?</p> <p>e. If the recipient is in the US, have they signed up to the Safe Harbour rules?</p>
9. Other considerations	<p>a. Have we considered the security of our payment systems and what measures do we have in place?</p> <p>b. Have we considered any data protection issues when working in collaboration?</p> <p>c. Have we considered the data protection arrangements for services we have outsourced?</p> <p>d. Do we continue to monitor DP arrangements as we update our IT arrangements? eg move to the cloud, permit staff to use their own devices for work purposes?</p>

This guide was produced in collaboration with:

Bates Wells Braithwaite is ranked by Chambers and Legal 500 as the leading charity and social enterprise lawyers in the UK. Our lawyers are personally committed to the charity sector, holding at least 60 trusteeships and sitting on many sector committees and commissions.

Our extensive client base includes service providers, grant-making foundations, philanthropists, public authorities and campaigning organisations. Their diverse causes span the world of voluntary endeavour, including aid and development, human rights, animal welfare, social housing, science, health and social care, the arts, the environment, minorities, faith and worship, community development and regeneration, and education.

Our specialist legal services for charities include:

- Establishment and registration of new organisations including charitable incorporated organisations (CIOs)
- Fundraising and tax advice
- Governance
- Internal disputes
- Advice on grants and contracts
- Restructuring – from incorporations through to mergers and group re-organisations
- Compliance and regulatory work
- Political activities and campaigning
- Public procurement and state aid
- Social finance

Charities are also at the heart of many of our other practice areas and teams. From employment to property to dispute resolution, BWB is capable of meeting the diverse and specialised needs of your charity.

For more information or to discuss how we can help your charity, please see our website: www.bwblp.com

This guide was kindly sponsored by:

Running a not for profit organisation effectively is a challenging task in the current economic climate. The right professional advice can make all the difference, with the combined pressure of raising funds, managing your finances, meeting stakeholder demands and keeping on top of the constantly changing regulatory and legal framework.

Kingston Smith can help you meet all these challenges by delivering a comprehensive range of services specially tailored for the not for profit sector including auditing, accountancy, VAT and fundraising.

Kingston Smith have a multi-disciplinary, dedicated not for profit team which acts for over 700 charities and not for profit organisations of all types and sizes including:

- Grant giving trusts and foundations
- Arts and culture
- Overseas Aid
- Disability charities
- Religious organisations
- Medical/health
- Education

We can help your organisation develop and achieve its aims and objectives and will provide you with the right advice at the right time. We do this by providing you with a partner who is accessible, who will take the time to understand your organisation and who will lead a dedicated client service team to help you meet your objectives.

For more information or discuss any business issues, please see our website: www.kingstonsmith.co.uk/

This guide, having taken into account the different ways in which the charity sector works, aims to help you understand what the law on data protection means for your charity. CFG has worked with the Information Commissioner's Office (ICO) (the body responsible for ensuring data protection compliance in the UK) to bring their best practice notes to your attention, in addition to a number of other useful resources which will provide you with further information.

Data protection matters for all charities. Not only is there the potential for the imposition of a civil monetary penalty or other enforcement action from the ICO, but the potential for reputational damage to charities is huge. The voluntary sector depends upon the trust of the public, but it is difficult to ensure we're 100% secure at all times. Therefore it is important for charities to be able to demonstrate that they are aware of their responsibilities to keep the data they hold secure, and that they are taking proportionate measures to protect personal data from misuse.

About Charity Finance Group

Charity Finance Group (CFG) is the charity that seeks to raise the standards of financial management in the voluntary sector by championing best practice, campaigning for a better operating environment for charities, providing high quality training and events and challenging regulation which hampers effective use of charitable funds. CFG has more than 2000 members, all senior finance professionals working in the sector and collectively our members are responsible for the management of over £19bn in charitable funds.



£25.00