Data Protection Action Group

A Document of Guidelines in Response to Concerns of Members of the Researchers in Fundraising Special Interest Group Regarding Prospect Research and the Data Protection Act

November 2004

Co-Chair: Robin Jones, Milestone Research
Co-Chair: Wendy Baverstock, Action Planning

Members

Judith Alldred, Imperial War Museum
Elly Boheme, Search and Prosper
Gail Bredis,
Finbar Cullen, Children's Hospice South West
Corrie Darker, the Healing Foundation
Liz Dixon, Victoria & Albert Museum
Amy Firth, World Society for the Protection of Animals
Christine Jeffrey, University of Oxford
Margaret Martin, Action Planning
Tracy Ogden, National Galleries & Museums of Wales
Barb Taylor, University of the Arts London

INTRODUCTION

This document has been created as a result of a group of prospect researchers from non-profit organisations coming together through the Institute of Fundraising to address concerns raised by prospect researchers regarding compliance with the Data Protection Act 1998 (the Act) specific to their job role. It has been assessed by experts in the field (please see bibliography) and then used by prospect researchers in a work environment to ensure accuracy and practicality. This document is by no means exhaustive and is representative of the main issues faced by those conducting donor and prospect research.

This document is not an explanation of the Act and does not cover all aspects relating to fundraising as a whole. For this, please refer to the Information Commissioner at Wycliff House, Water Lane, Wimslow, Cheshire, SK9 5AF or www.informationcommissioner.gov.uk and the Institute of Fundraising's Codes of Fundraising Practise available at www.institute-of-fundraising.org.uk

The main aim of this document is to assist prospect researchers when confronted with ambiguities within the Act which have a direct bearing on their role within the fundraising effort in their organisation. It is intended that this is for guidance only and should be used as a practical tool in enabling prospect researchers and others responsible for donor/prospect research to develop their own policies and procedures, which can be incorporated into their Data Protection Policies and Procedures for fundraising as a whole. If organisations are in any doubt as to their obligations under the Act, they should seek legal advice.

With knowledge sharing and practicality in mind, this document has been laid out in three sections; Data Collection, Data Processing and Data Sharing, with a miscellaneous section to cover issues such as liability and training. Within each section is a question or statement raised by members of Researchers in Fundraising as being of main concern. This question or statement is then clarified and answered and is accompanied by a relevant example or case study and then several ideas for best practice guidelines. There is also a set of appendices with suggestions for forms and wording for things such as opt in/out e-mail and Subject Access Request forms.

While it is understood that the Information Commissioner is not in a position to endorse every individual set of guidelines created by groups for their members, it is hoped that this document, when taken with the Institute's own guidelines for fundraising as a whole, will be seen as a genuine and concerted attempt to ensure that prospect research is undertaken with the spirit of the Act at heart and as an example of the professionalism of Prospect Research and its significant role in the fundraising effort.

CONTENTS

1. DATA COLLECTION

1.1. Obtaining consent from new prospects 3
1.2. Time scales for obtaining consent and holding data 4
1.3. Researching prospects suggested by volunteers either UK or abroad 5

2. DATA PROCESSING

2.1. Data retention and archiving 6
2.2. Personal data, sensitive personal data and the public domain 7
2.3. Prospect research consultants 9
2.4. Non-computerised databases 10

3. DATA SHARING

3.1. Request by donor/prospect for information held 11
3.2. Contracts between clients and prospect research consultants 12
3.3. Exchanging supporter data with overseas associates 13

4. GENERAL

4.1. Data controllers/processors and liability 14
4.2. The Data Protection Act and Information Management knowledge 15
4.3. Reconciling conflicting advice 16

5. BIBLIOGRAPHY 16

6. APPENDICES

6.1. Data Protection principles and schedule conditions 17
6.2. Suggested opt-in and opt-out formats 20
6.3. Staff confidentiality agreement 21
6.4. Sample e-mail disclaimer 21
6.5. Subject Access Request Form template 22

1. DATA COLLECTION

1.1. Obtaining consent from new prospects

Question:
How is it possible to obtain consent from a prospect to collect and process data on them, when research has to be done before we can establish whether they would be interested in supporting our cause and where to contact them?

Answer:
The Act does not clearly state to what degree fundraisers may develop a file when researching prospects before disclosure and consent become necessary. It is considered appropriate that, providing all principles of data processing are being followed, a declaration is included within the first formal or written contact.

Example:
You have compiled a list of prospects including a name, contact address, wealth and sympathy for your cause to present to your fundraisers as possible invitees to a major pledge event you are holding. Providing this information has been collected fairly, is not excessive for the purpose and does not contain sensitive data, this is acceptable. The fundraiser must ensure that a declaration giving the prospect an opportunity to opt-out is included in the invitation to the event.

Best Practice:
- Ensure that the fundraisers and volunteers who are making the first contact with a prospect are fully informed of their obligation to obtain consent for the continued processing of personal data.
- The first formal contact is often an invitation to an event. RSVP cards should include an appropriate disclaimer, allowing the prospect to opt-out.
- If the prospect does opt-out, all extraneous information must be removed, apart from skeletal details which allow it to be seen they have opted-out and should not be contacted.
- Implement a mechanism for tracking whether consent has been obtained with reminders for researchers, fundraisers and volunteers regarding their obligations under the Act.
- Aim to ensure at all times that the information being processed about a data subject is necessary for the legitimate interests of your organisation. It is recommended that personal data only be processed if there is a specific purpose for that data, in support of fundraising activities.

1.2. Timescales for obtaining consent and holding data

Question:
How soon do we have to obtain consent from prospects and donors to process their data and how long can we keep it for?

Answer:
Question 1.1 shows that consent should be obtained as soon as the first contact is made. It is impossible to put a timescale on this, however if the data is being processed for a specific purpose, in support of fundraising activities then there should not be an issue of waiting too long to obtain consent. The Act states that data should not be kept for 'longer than is necessary'. Fundraising campaigns can run for long periods of time, as much as several years, and are likely to entail the development of relationships with some prospective donors over a correspondingly long period, however, consent should still be obtained at first contact and can be kept for as long as your organisation can justify its necessity.

Example:
You are working on wealth information for a group of prospects suggested to you by a volunteer as possibly being interested in the capital campaign you will be beginning next year. Providing the data is being processed in accordance with Data Protection principles and consent is obtained at first contact, this is acceptable. However, to comply with the principles, it is necessary to ensure the data is accurate therefore any such work done before it is immediately needed should be re-checked and updated before any decision regarding contact with the prospect is made. If the data is held for up to year without being used, its reasons for being processed should be checked and if still valid, then the data should be updated.

Best Practice
- Regularly review how long it has been since consent has been obtained and for what purpose, ensuring your organisation and the data subject is aware if the purpose for the data processing has changed.
- Data storage policy should include specific criteria by which a potential data subject qualifies before data is stored.

1.3. Researching prospects suggested by volunteers either in the UK or abroad

Question:
How do we reconcile issues of consent when researching prospects whose name has been given to us by a volunteer/board member?

Answer:
Question 1.1 shows that consent should be obtained as soon as first contact between the organisation and the prospect is made. This is regardless of whether the prospect has been identified by the prospect researcher, the fundraiser, or the volunteer. As in Question 1.1 preliminary research can be done, providing that your data collection process is following the main principles of data protection. This is also the case when researching prospects who do not reside in the UK.

Example:
Your Appeal Chairman is good friends with a high profile businessman who he thinks may be a good prospect. He has suggested the name to you and, after doing some preliminary research, you discover he had dinner with him this week and told him about the cause, offering to involve him further by meeting with one of your fundraisers. It may be unrealistic and inappropriate to expect your volunteers to broach data protection when they first discuss the cause with the prospect; however, when you pass your research to your fundraiser to enable them to engage the prospect by inviting them to a meeting, you should make sure that any letter or verbal invitation contains a data protection statement.

Best Practice:
- Ensure that you have a simple data protection statement that can be easily added to written invitations or included in a conversation with a prospect. A simple statement will ensure that is used more often.
- Be clear among your organisation if you will be obtaining other forms of data protection consent at this time e.g. electronic communications consent or sensitive personal data consent.
- Make sure that your volunteers are aware of the organisation's obligations under the Act.
- Develop and implement a section within your organisation's data protection policies and procedures that prescribes at what stages in the fundraising process consent should be obtained and in what ways to ensure consistency.

2. DATA PROCESSING

2.1. Data retention and archiving

Question:
The legislation states that data must not be stored indefinitely. How long are we allowed to store personal information and what should we do when the data is no longer useful?

Answer:
Financial data must be stored for 7 years for auditing purposes. Outside of that, personal information storage must follow the main principles of data protection, namely that data collected for a purpose should not be kept for longer than is necessary *for that purpose*. Data protection legislation is there to protect the data subject, not the controller or processor and as such it is important that you have justifications in place within your organisation for keeping a prospect's personal information. For fundraising purposes, campaigns/appeals are a good yardstick for this. They are a specific purpose and often have specific timescales attached. Because campaigns and appeals often last for several years, it is important to have mechanisms is place to ensure the personal data is kept accurate regularly.

Example:
Your three-year campaign for funds to refurbish your library is coming to an end. During those three years, you and your fundraisers and volunteers have identified many possible names, lots of who became prospects (from which consent was obtained) and some of whom became donors, and which your organisation now has relationships with. Now that the purpose for which this data was stored is over, it is important to assess whose personal information you can keep and whose you need to remove. Personal information on donors obviously needs to be kept and should be maintained in the normal way to ensure accuracy. Any prospects who agreed to have their information processed and indicated that they would be interested in keeping up to date with your work, even though they were unable to support at the time, can also be kept. If you have personal information left relating to people who showed no interest in your campaign or appeal then it should be removed, ensuring that skeletal information remains if they refused consent or indicated that they did not want to be contacted.

Best Practice:
- Devise a system which enables you to see when personal data might be losing accuracy and how to update it.
- Include your data protection policies and procedures for keeping personal data within any strategy paper written for a particular campaign or appeal.

2.2. Personal data, sensitive personal data and the public domain

Question:
What is the definition of the public domain in this context and what information found there can I legitimately use for prospect research?

Answer:
The general definition of data in the public domain is data that can be appropriated by anyone, such as that found in newspapers, magazines, journals, reference books such as Who's Who, buyable mailing lists etc. This is broader than the official, legal definition of 'public domain' which refers to data no longer covered by copyright legislation. When using any data in the general public domain, controllers and processors must still abide by whichever copyright law is applicable. Guidelines from the Information Commissioner to the Institute of Fundraising state that personal data found within the public domain can legitimately be used for prospect research, however what is not clear is how applicable this is to sensitive personal data.

For the purposes of the Act, sensitive personal data is data that falls into the following categories: Racial/Ethnic origin; Political beliefs; Religious/similar beliefs; Trade Union membership; Physical/mental health condition; Sexual life; Commission or alleged commission of an offence and any proceedings such as a court sentence. Wealth and salary is not considered to be sensitive personal data. Data of this sort can only be legitimately processed in two ways:

1. With the explicit "opt-in" consent of the data subject, above and beyond the consent you obtain for the processing of personal data.
2. If one of the other 11 conditions are fulfilled (see appendix 6.1), although if explicit consent is refused, it does not matter if the sensitive personal data fulfils one of the other conditions.

For the purposes of prospect research, condition 5 is the most relevant as it allows the processing of sensitive personal data which the data subject has "deliberately made public". The task of the prospect researcher is to ensure that any sensitive personal data discovered through their research is "from the horse's mouth". This may include making judgements on whether a newspaper article about a prospect is an interview or just a piece written about them. Journalism is excluded from following data protection rules, therefore just because it has been printed in the press, it does not necessarily follow that the data subject has made any sensitive personal data contained within it "deliberately public".

Sensitive personal data told to your organisation does not equate to either "deliberately public" or "explicit consent" unless you confirm at the point of receiving that data that they are happy for you to process it. For example, if a prospect tells you they are particularly interested in your cancer charity because they had suffered leukaemia as a child, you would need to tell them that you wished to store that specific sensitive personal data and obtain their consent to do so.

Care must also be taken when processing data from which sensitive personal data can be implied. This whole area is very subjective and as such, several examples have been provided.

Example 1:
While researching a prospect, you discover in their Who's Who entry that they have been awarded a KSG. Further research shows that this makes him a Knight of the Order of St. Gregory; an award only given to those who have shown consistent commitment and dedication to good works within the Catholic Church. One of your fundraising volunteers is also a high-profile Catholic and may be able to make an introduction. Can you process this implied sensitive data about their religion?

Yes. They chose to include their award in their Who's Who entry and hence have made this implied sensitive data deliberately public.

Example 2:
You are an organisation that provides printed information to people who request to be kept up-to-date on medical research into diabetes. While there is nothing on your database to definitively identify any of these people as diabetes sufferers, it can be implied that the likelihood is that a large majority of them are diabetic. You are about to share your information with a database mining agency. Is there a possible data protection infringement?

If the suggestion is that the database member is, in fact, diabetic, then the data showing them to be on this mailing list must be treated as sensitive and the data subject must have given their explicit consent for both your processing of it and the sharing with a third party. If, however, you feel the implication cannot be justified then the standard rules would apply as if the data was merely personal and not sensitive. Either treat it as sensitive and use the request from the data subject to be on the mailing list as a point at which to obtain explicit consent, or choose to process the data in a less revealing way, e.g. by giving each mailing list a code from which it cannot be implied what information they are receiving.

Example 3:
Red Star Research states that a major prospect has given over £500,000 to a political party over the past year. There is no quote from the supposed donor to back this up. Can we process this without the prospects political beliefs being implied?

Yes. Although Condition 5 does not really apply in this particular case as it cannot be shown that this is information the donor has made "deliberately public", it is also proven that many businessmen/women will merely donate to the party that is in power to keep in with the government of that day rather than because of their political affiliations hence there is no real implication at all.

Note
Issues of storing sensitive personal data for the purposes of keeping fundraisers/volunteers safe from harm is not within the remit of this document and guidelines should be developed and included within data protection policies for your organisation as a whole.

2.3. Prospect research consultants

Question:
Are there any extra data protection responsibilities for consultants who do prospect research on behalf of an organisation?

Answer:
Consultant prospect researchers should follow all the same guidelines as internal prospect researchers when collecting and processing data. Where the difference comes is in the contractual arrangement between the consultant and the organisation, such as who "owns" the data, who is responsible for it as "data controller", what should consultants do with the personal data once they have passed it to the organisation they collected it for and what arrangements are in place to ensure data security during transfer. Contractual arrangements between a consultancy and an organisation should be done on a case-by-case basis, using these guidelines as a way of ensuring that relevant agreements regarding data are reached. Consultancies should have their own Data Protection policies and procedures which they can refer to when making arrangements with clients.

Example:
Your organisation has provided access to its database for a data mining agency to analyse to see if you have any potentially valuable prospects within your membership. Ask to see the consultant's policy regarding data. Use your own policies and procedures to come to a written agreement with the consultancy on issues such as data ownership, return of data provided, processing of the new information found etc. and when in doubt always seek legal advice as it will be the organisation who is responsible for any data they provide to the consultancy.

Best Practice:
- Consultants should devise an appropriate policy statement for their organisation.
- Consultants should be responsible for making clients aware of the policy.
- The Consultancy should be responsible for ensuring the policy is adhered to within the organisation and that all staff are adequately trained and supervised on managing the policy.
- The policy should include points and guidelines such as:

  The return of any data provided by a client when the project is completed or within 3 months

  Secure destruction of client data after the project closes (6 months seems to be the suggested time scale)

  Maintenance of prospects researched recorded within the consultancy.

  No client data should be exchanged with any other client/person.

  Data received from a client should not be duplicated or reproduced in any way.

  Data should be stored securely at all times.
- The Institute of Fundraising has established a working party to address special issues regarding data in the relationship between consultants and their clients. This should be your first port of call if you are looking to form a contract.

2.4. Non-computerised databases

Question:
Our organisation doesn't have a computerised database and our prospect research is processed manually. What are our obligations under the Data Protection Act?

Answer:
The main change between the 1984 and 1998 Data Protection Acts was the extension to include manual data. This means that even those not using computers must abide by the eight main data protection principles. The difference comes when looking at the ease with which personal data is found within the system that you use; the key phrase being "relevant filing system". Your filing system is deemed to be relevant if:

a. The files forming part of that system are structured or referenced in such a way as to clearly indicate at the outset of the search whether specific information capable of amounting to personal data is held within the system and, if so, in which file or files it is held.

b. It has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where, in an individual file/s, specific information can be readily located.

The recent case of Durant vs. the FSA made a key distinction in terms of chronological paper files. If you keep personal data in paper files in no discernable order other than by date, it is not deemed that an individual could be easily identified from it and so is not 'personal data' in terms of the Act. This ruling is currently being appealed however and the position may change.

Example:
Your organisation is mostly staffed by volunteers who are not necessarily brilliant on computers and so you have a paper filing system where files are stored alphabetically and within each file there are dividers marking sections to indicate where relevant information needs to go e.g. contact details, correspondence, gift aid forms etc. In terms of the Act, this is a sophisticated means of readily indicating where specific information can be located and as such is as liable to the Act as a computerised database.

Best Practice:
- Do an internal audit to determine if your filing system is "relevant" and, if so, develop appropriate data protection policies and procedures to govern it.
- Always keep the interests of the data subject at the forefront of any data processing decisions.

3. DATA SHARING

3.1. Request by donors and prospects for their information

Question:
What should we do when a prospect or donor requests to see all the personal data we have processed regarding them?

Answer:
A hard copy of all their personal data held either electronically or in paper form, must be supplied within 40 days from receipt of a written request from the data subject. There are some exceptions to this but they should be covered by your organisation's overall data protection policies and procedures. You are within your rights as a charity to ask for an administration fee of up to £10.00. This very specific type Subject Access Request of is not the same as a supporter asking for details on how much money that have donated over the past year or other specific pieces of information. See appendix 6.5 for an example of a standard Subject Access Request form you might provide to a donor or prospect asking for you to provide the personal data you hold on them.

You only have to supply data that refers directly to them and from which they can be identified and hence can be seen as infringing their privacy. You do not have to supply any data which contains information regarding other data subjects, as this would be a breach of their privacy rights, or you can prove that "disproportionate effort" would be required. In most cases, a data subject's rights to access their data is something that should be dictated at the highest level of your organisation with policies and procedures that cover all your departments e.g. development, marketing, press etc.

Example: Quoted from Ticher, Paul (2000) 'Data Protection for Voluntary Organisations', *Directory of Social Change in association with Bates, Wells & Braithwaite* pg. 57

You work in a mediation service that does not always manage to win the trust of potential clients. Some of them start to make Subject Access Requests in order to 'see what people are saying about me.' You decide on a twofold strategy. Firstly, most of the records will be kept in paper files. Clients who have agreed to work with the service each get their own file, but until then, the information is not systematically filed or readily accessible, and therefore, not personal data. Secondly, the service will extend its policy on confidentiality, to make it clear that information provided by or related to other people will never be disclosed without their consent.

Best Practice:
- Make sure that staff are aware of the legal status of a Subject Access Request so they deal with it relevantly
- Make sure that all prospect research is correctly sourced and referenced
- Liase with those responsible for policy within your organisation about how the issue is being addressed at organisational level.

3.2. Data transfer and security

Question:
I often pass personal data on prospects around the office to fundraisers and also to volunteers. What should I be doing to ensure the personal data is processed fairly and is secure?

Answer:
It is important that your data protection policies and procedures include detailed instructions as to how this should be done, basing them on the eight principles of data protection, especially regarding taking appropriate steps to protect the data from loss or damage and ensuring that where the data is going has equally adequate security in relation to personal data processing. This question is best answered with best practice ideas, extensive examples of which can be seen below.

Example:
An ex-colleague who has moved to another organisation calls you. They have been given a name by a volunteer that they remember as being a supporter of the organisation that they used to work for. They had already done lots of work on them and had kept good records of the relationship between the supporter and fundraisers and want to know if you can e-mail them the work they did. To do so would be compromising their data on several counts. Firstly the personal data processing they gave consent for was for your organisation, not another. Secondly, it is your data controller's responsibility to ensure that the security of personal data is not compromised by either being seen by someone who does not have consent or by being lost or damaged during the process of e-mailing. You would have to tell your colleague no.

Best Practice:
- Ensure all prospect research profiles and other information concerning prospects in electronic and paper form are clearly sourced, dated and marked "CONFIDENTIAL".
- The documents and/or emails should clearly state for whom the information is intended.
- A standard email disclaimer can be found by clicking here
- Consider password-protecting raw data (e.g., in the form of databases or zip files) and prospect profile documents that are transferred electronically.
- Have a method of storing the data securely and centrally – e.g., in a database which is accessible only by password and in files which are locked in cabinets in locked rooms, with the keys safely held.
- Prospect information should remain within the fundraising office and not taken home.
- When colleagues take profile reports with them to meetings and events remind them not to bring them out at such meetings/events, nor leave them anywhere but on their own person. They should return the reports to the central filing system or Researcher as soon as possible after the meeting/event.
- Researchers and fundraisers should give careful thought to the content of the profiles in terms of for whom and what they are intended. For example, an event for 200 people where prospect research reports may be provided to a large number of the fundraising team and volunteers should contain a lot less data (and potentially sensitive data at that) than a top level ask meeting between a prospect and the Chief Executive.
- Ideally all members of the team should have a good level of understanding of the Data Protection laws and what they need to do to implement them correctly. To help with this you may be able to persuade management to provide the team with in-house or out-sourced training, and you can encourage colleagues to refer to these guidance notes.

3.3. Exchanging supporter data with overseas associates

Question:
We have an American Friends scheme and there are sometimes overlaps between prospects we are working on. What are the rules regarding exchanging personal data with organisations overseas?

Answer:
The eighth principle of Data Protection requires that "Personal data shall not be transferred to a country or territory outside the European Economic Area [EEA], unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data". At time of writing (October 2003), the EEA countries are the 25 EU Member States, and Iceland, Liechtenstein and Norway. It should be remembered that the Channel Islands and Isle of Man are not (at October 2003) part of the EEA.

Some countries outside the EEA will be designated as "adequate" by the European Commission and will appear on the IC's EU Approved List, which can be accessed via the News & Events section of the IC website. At October 2003, these are Switzerland and Hungary. Also Canada, as long as the transfer of personal data falls within the Canadian Personal Information Protection and Electronic Documents Act 2000.

The USA has no general data protection law and so is not designated as adequate by the EC. However, the EC and the US government have drawn up a "Safe Harbour" agreement, whereby US organisations and businesses may commit themselves to comply with a set of data protection principles and become members of the Safe Harbour scheme. Any organisation that is a member of the scheme is deemed as providing an adequate level of protection for transfers of personal data to the US from EU member states, and therefore provides the basis for compliance with the Eighth Principle of the DP Act in the UK. Members who have signed up to the Safe Harbour agreement can be found at www.export.gov/safeharbor/

Even if a country has not been designated as adequate by the European Commission, a data controller can nevertheless come to their own conclusion that the country provides an adequate level of protection for a particular transfer or set of transfers. Your organisation should have made provisions for this within their overall data protection policies and procedures.

There might also be other cases where the nature of the data and the circumstances of the transfer coupled with the data controller's knowledge of the country of transfer and the particular recipient mean it is reasonable to conclude there is adequacy without the need for a detailed analysis. For example, a transfer of a list of names and addresses for a mailing may be fine, as long as the data is only held by the overseas processor for the time required to undertake the mailing, and is then destroyed or returned to the UK. There are several exceptions whereby data controllers can transfer personal data even if no adequate protection exists. For example if the data subject has given consent for the transfer of their data. Again this is an area where examples of best practice are the best answers and some are detailed below.

Best Practice:

- Process and transfer your data to comply with the other seven Data Protection Principles.
- Follow the guidance given in the rest of this document.
- Note there are no extra restrictions to the transfer of data to EEA countries.
- Keep up-to-date with the list of EEA countries, and other countries designated to have adequate protection by the European Commission – see IC website for regular updates.

4. GENERAL

4.1. Data controllers, processors and liability

Question:
Are data controllers completely liable if it is data processors that do the day-to-day collection and storage?

Answer:
It is important to be clear about the definition of data controller and data processor. Unless it is a sole trader, the data controller is usually an organisation which is comprised of all individuals employed within that organisation who handle personal data. The term data processor generally refers to external agencies. It is the responsibility of the data controller to put in place adequate security arrangements and have a written agreement drawn up to prevent the unauthorised or unlawful processing of disclosure of data by the data processor. Anyone processing personal data must comply with the eight principles of data protection therefore all employees within an organisation have a personal responsibility to comply with the Act.

Although breaches of the Act can be committed at a personal level and individuals can be personally liable for criminal offences, for example unlawful disclosure of information about an individual or misuse of data such as using someone's credit card information for personal gain, it would usually be the organisation as a whole which would be liable rather than the individual data handler. The Information Commission would most typically check DPA procedures with an organisation's nominated representative, rather than seeking out the individual who may have (perhaps unwittingly) breached the Act.

Best Practice:

- Data Protection self-audit to ensure where the strong and the weak points are.
- A written Policies and Procedures manual for DP compliance that could even be part of a database policy & procedures manual.
- Accurate sourcing and dating of prospect information, possibly with a disclaimer involved as well as a mechanism for updating or deleting irrelevant information.
- Regular in-house training to ensure all staff that use information within an organisation are aware of the legislation. This could include teaching trustees and development boards.
- Making sure that the organisation is compliant with copyright law at the same time.
- Only hold information on an individual that is absolutely relevant and objective - rule of thumb: how would you feel if you read that information about yourself?
- If sensitive information has to be conveyed, do it verbally.

- Implement a system on your database where, when you add a name to your records, you give both the point of acquisition (i.e. staff member or trustee who identifies someone as a prospect) and the reason for adding that person.
- Always date and source information on a database and in a written prospect profile.
- Keep all data secure through use of locked cabinets, locked doors, password-protected files and databases.
- Don't leave database records and prospect profiles open on your PC whilst you are away from your computer.
- Don't leave paper files and prospect profile documents lying around unattended.
- Mark all research profile documents as "STRICTLY CONFIDENTIAL" and distribute only on a need-to-know basis. Encourage users of your documents to return them to you once they have finished with them so that you may either store them securely or shred them.
- Don't include information in your research profiles which is excessive to need.
- If you have a doubtful source for a piece of information, try and find another more credible source to corroborate it. If still in doubt, make a decision either to omit the piece of information, or to retain it with a caveat on the source.

4.2. Prospect research and information management knowledge

The legalities of data management should be a priority within organisations to ensure that all those involved in the collection, collation, analysis and storage of information regarding people are sufficiently trained in these issues. The key is making sure new researchers are informed as quickly as possible about the legislation governing the information they will be collecting and using and that experienced researchers are encouraged to keep their knowledge up-to-date and set examples wherever they work.

- Charities and consultancies should use interview questions to assess research candidates' knowledge of information management legislation. This will encourage charities to organise training for new recruits without experience of the area and also encourage more experienced researchers to keep on top of their IM legislation knowledge.

- The Institute of Fundraising should publish a set of best practise guidelines endorsed by themselves and the Information Commissioner to ensure a consistency of standard across all voluntary organisations

- DP training should be given as much importance as other company policies within the induction process for researchers new into a role. This may include a session with the in-house expert or with the charities legal team and should take place within the first month of employment. Researchers with no experience of data protection might also wish to be placed on an external training course or to be taught using the IC online seminars as early in their role as possible. As well as helping those new to fundraising research it should encourage organisations to have a DP expert or for their legal team to brush up on information management legislation areas.

- Any organisation with a database should have a working Policies and Procedures manual that has data protection (and copyright) compliance at the heart of its instructions. This will help eradicate any bad habits picked up by anyone in the organisation, not just researchers, and could help ensure that a culture of 'day to day' correct management of data is cultivated.

4.3. Reconciling conflicting advice

It would be too simplistic to hope that one action alone can reconcile the huge volume of information on data protection which confronts prospect researchers. Instead we need to take a number of steps to ensure that we adhere to the Act in a sensible, ethical yet workable way. What follows is an initial list of recommendations and steps which can help to reconcile information on the Act:

- The formation of the Researchers in Fundraising Data Protection Action Group has been a significant step in trying to make sense of the DPA for prospect researchers. The development of this document has gone a long way in addressing some of the concerns Group and questions that fundraising researchers have, regarding the DPA and has also highlighted key gaps in understanding of the Act among voluntary organisations as a whole.

- The issues covered in this document are by no means exhaustive and have deliberately been written with prospect research in mind. The detail which has been required for this document may go some way to demonstrating what level of detail may be required for similar guidelines for other Special Interest Groups.

- This document needs to become part of a greater whole that offers detailed and pragmatic advice to fundraising departments in general. If in doubt regarding any aspect of data protection compliance, prospect researchers must seek advice from their organisation's legal and policy decision makers.

5. BIBLIOGRAPHY

http://www.keepinglegal.com

http://www.informationcommissioner.gov.uk

http://www.hmso.gov.uk/acts/acts1998/19980029.htm.

Experian 'Data Protection Act 1998 – A simplified guide to assist businesses holding personal information on customers, suppliers, directors, shareholders or others' (no date), Experian Information Services Division

Institute of Fundraising Codes of Practice: Data Protection

Lee, Stephen, (2002), 'Between a Rock and a Hard Place: The impact of the implementation of the Data Protection Act 1998 on United Kingdom fundraising and direct marketing practice.' New Directions in Philanthropic Fundraising, 33 (3), USA.

Ticher, Paul, (2000), 'Data Protection for Voluntary Organisations' Directory of Social Change in association with Bates, Wells & Braithwaite.

APPENDIX 6.1

Data Protection Principles
There are eight principles put in place by the Data Protection Act 1998 to make sure that information is handled properly.

They say that data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with the data subjects' rights
7. Secure
8. Not transferred to countries without adequate protection.

By law data controllers have to keep to these principles

Conditions for Processing Personal Data (Schedule 2)
1. The data subject has given his consent to the processing.
2. The processing is necessary-
   (a) for the performance of a contract to which the data subject is a party, or
   (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary-
   (a) for the administration of justice,
   (b) for the exercise of any functions conferred on any person by or under any enactment,
   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. - (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
   (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Conditions for Processing Sensitive Personal Data (Schedule 3)

1. The data subject has given his explicit consent to the processing of the personal data.
2. - (1) the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
   - (2) The Secretary of State may by order-
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary-
   (a) in order to protect the vital interests of the data subject or another person, in a case where-
      (i) consent cannot be given by or on behalf of the data subject, or
      (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
4. The processing-
   (a) is carried out in the course of its legitimate activities by any body or association which-
      (i) is not established or conducted for profit, and
      (ii) exists for political, philosophical, religious or trade-union purposes,
   (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
   (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
6. The processing-
   (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   (b) is necessary for the purpose of obtaining legal advice, or
   (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. - (1) The processing is necessary-
   (a) for the administration of justice,
   (b) for the exercise of any functions conferred on any person by or under an enactment, or
   (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
   (2) The Secretary of State may by order-
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified,
   (b) provide that, in such cases as may be specified, the condition in sub paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. - (1) The processing is necessary for medical purposes and is undertaken by-
(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. - (1) The processing-
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

APPENDIX 6.2

Suggested Opt-in and Opt-out Formats

The **>>charity name<<** values your support and promises to respect your privacy. The data we gather and hold is managed in strict accordance with the Data Protection Act (1998). We would like to keep you informed about the vital work we do, if you do not want to receive this information please let us know by ticking this box□.
We may, from time to time, share personal information supplied by you with other organisations with similar aims to >>**charity name<<** If you do not wish us to share personal information supplied by you with other sympathetic organisations, please let us know by ticking this box □.

The >>**charity name<<**holds and manages the data we gather in strict accordance with the Data Protection Act (1998).
We wish to keep you informed about the vital work we undertake with the funds you raise, if you do not want to receive this information please tick this box □ and return to the address below. We may share information (never financial) supplied by you with organisations who have similar aims to >>**charity name>>,** if you do not wish us to share this information please tick this box □ and return to the address below.

We would like to keep you informed about events and how your valuable donations are being spent on >>**charity name<<**If you do not wish this, please tick here□.

The most cost-effective way for us to contact you with updates on the vital work of the **>>charity name<<** is by email. Please print your email address clearly in the box provided.

APPENDIX 6.3

Staff Confidentiality Agreement

You have a duty of confidentiality to **>>charity name<<** both in common law and by virtue of your contract with your agency and by statute. This applies not only during the course of assignment with **>>charity name<<** but also after the assignment has ended. This confidentiality clause covers such matters as knowledge of **>>charity name<<** business, clients, business contacts, supporters and procedures.

You will not disclose to, or use for, another organisation's or individual's benefit any confidential information that you have or continue to acquire.
All manual and electronic records relating to organisations and individuals and their relationship with **>>charity name<<** are deemed to be confidential. They remain the property of **>>charity name<<** irrespective of the originator, the purpose for generation, their location and the means by which they are held. You have a duty of care to ensure these records are used in an appropriate and secure manner at all times.

If you fail to comply with the standards above, **>>charity name<<** will end the assignment, and as it deems appropriate raise a complaint about you to your agency, notify other agencies of your breach, take legal action against you and or your agency for any damage or loss the organisation incurs and report the breach to the Data Commissioner.

Please use block letters

Name……	Position……
Signed……...	Department……..
Location……	Dated……

APPENDIX 6.4

Sample E-mail Disclaimer

If you have received this email in error and are not the intended recipient please notify the Email Administrator using the email address: **>>insert link to your IT department's email address<<** Please note that access to this email by anyone other than the intended recipient is unauthorised, and we would appreciate you respecting our privacy. Any disclosure, copying or distribution of a message by an unintended recipient may be unlawful.

>>Charity name<<
>>Charity registration<<
>>Subsidiary Companies, if any<<
>>Registered charity address<<

APPENDIX 6.5

Subject Access Request Form

Under the terms of the Data Protection Act 1998, an individual is entitled to ask >>**charity name**<< for a copy of all of the personal information that the organisation holds about him/her.

If you would like a copy of the information that >>**charity name**<< holds about you, please answer the following questions and return to the Data Protection Officer at >>**charity name**<< at the address below.

SECTION 1: PERSONAL DETAILS

Name:

Address:

Postcode:

Length of time at this address:
(years)

Telephone Number: Fax Number:

Email:

Are you the individual named above? YES / NO (please circle)

If you are not the individual named above, but you are acting on their behalf and with their authority (for instance the individual's parent, guardian, or legal representative), please send a written copy of this authorisation with the completed form.

SECTION 2: LOCATING YOUR INFORMATION

To help us locate your information, please tick if you have ever been:

A volunteer with (CHARITY NAME) □

A supporter of (CHARITY NAME) □

If you have not ticked any of the items in Section 2 then please tell us of any reason why you think we might hold information about you:

SECTION 3: DECLARATION

To be signed by the individual:

I confirm that I am the individual named in Section 1. I understand that it is necessary for >>**charity name**<< to confirm my identity and that it may be necessary to obtain more detailed information in order to locate the information that I have requested. If any of the information that I have given (e.g. address) is different to that which is held by >>**charity name**<<, I may be asked for additional identification

Name:

Signature:

Date:

To be signed by person(s) acting on behalf of the individual named in Section 1.

I confirm that I am acting on behalf of the individual named in Section 1 and that I have submitted proof of my authority to do so.

Name:

Address:

Postcode:

Signature:

Date:

Please return your completed form to:

The Data Protection Officer……>>**appropriate address**<<……

>>**charity name**<< will respond to your request as quickly as possible. We aim to reply within three weeks, but we may take up to 40 days. We will send a copy of the information requested to the address provided in Section 1. We will send you a copy of all of the information that we hold about you, except information that also concerns another individual.