Who this paper is for

Many voluntary organisations – probably most – make use of volunteers to help them run the organisation or deliver their services. Volunteers often take on significant responsibilities. Some organisations are run entirely by volunteers; in others volunteers carry out tasks that are similar to those carried out by employees. These duties may well include handling information about people – clients, members, supporters or colleagues – on behalf of the organisation.

Whenever an organisation makes use of information about individuals, Data Protection considerations are likely to be important. This paper looks at the issues that arise and the kind of policies and procedures that may be required when volunteers are involved, in situations such as:

- where the volunteer works in the office, alongside paid staff;
- where client services (such as helpline advice or home visiting) are delivered by volunteers; and
- where the branches of an organisation are run by volunteers.

The paper is particularly aimed at:

- anyone who is responsible for managing, supervising, inducting or training volunteers.
- anyone who is responsible for recruiting volunteers, whether for their own organisation or for placement in other organisations.
- anyone who is responsible for providing guidance to local groups or branches run by volunteers.
- volunteers who run local groups or branches.
- the board of trustees in any organisation that makes use of volunteers.

When we talk about volunteers, this includes anyone who is not under contract, either as a direct employee or as an agency worker or contractor. It would therefore include people on work experience, student placement, internship and in similar situations.

The legal background

An organisation is “vicariously liable” for the actions of an employee. In other words, if the employee harms someone else in the course of their work, the injured party could take legal action against the employer, not the employee. The situation with volunteers is not quite so clear-cut. In most cases it would be necessary to prove that the organisation itself was at fault in some way; otherwise action could be taken against the volunteer themselves. (Note that for this reason the Russell Cooke Voluntary Sector Legal Handbook recommends that an organisation’s insurance should cover liabilities created by volunteers and indemnify them in cases where action is taken against them.)
Most information about people becomes “Personal Data” – and therefore subject to the Data Protection Act – as soon as it is recorded on a computer or in a filing system. (The situation with paper records, in particular, is technically complex but it usually makes sense to treat paper records on the basis that Data Protection applies to them as well.)

Any organisation that holds personal data must comply with the eight Data Protection Principles (see Appendix A). If anyone is harmed by a breach of the Principles they are entitled to claim compensation. And if there is a serious breach of the Principles – particularly if confidential information falls into the wrong hands – the organisation may face a penalty from the Information Commissioner of up to £500,000. In addition, of course, any breach of Data Protection might well bring adverse publicity, affecting the reputation of the organisation.

Compliance with the Principles is a legal obligation, but the Data Protection Act does not specify in any detail what steps you should take. It is up to each organisation to set out its own policies and procedures to ensure compliance, tailored to its own situation and its preferred operational practices.

**Data Protection and Confidentiality**

Data Protection has a very close relationship with Confidentiality, but they are not the same thing. Information about individuals that happens to be in the public domain is unlikely to be confidential, but certain Data Protection considerations would still apply. Meanwhile information that is not recorded – or that is recorded in a way that falls outside the strict definition of Personal Data – may well be confidential even though it is not technically Personal Data. Much of an organisation’s non-personal information may also be confidential.

Information about individuals is most often treated as confidential because there would be a risk to the individual’s well-being in some way if the information fell into the wrong hands or became public knowledge. A sound Confidentiality policy is therefore essential in most voluntary organisations, to protect clients and service users in particular, but also to respect the privacy of donors, supporters, employees and volunteers. In order to avoid confusion it is often best to separate this from the organisation’s Data Protection policy, while ensuring that the two policies are consistent with each other and mutually supportive.

Confidentiality means defining clear boundaries within which information will be held; in other words, who can access which information and for what purposes. It is not really enough just to say ‘this information is confidential’ without setting more explicit boundaries. At several points in the Data Protection Act there is reference to ‘authorised’ access to data. The boundaries set out in a Confidentiality policy provide an important part of the framework for authorising access.

Data Protection is a relatively recent innovation, but Confidentiality is a long-established legal concept. Employees have an implied contractual duty of confidentiality towards their employer’s information (whether or not the contract says so).
Volunteers do not have the same contractual duty, but they are subject to a common law duty of confidentiality. (If you are given information ‘in confidence’ you are legally obliged to keep it confidential.) In both cases – but especially if you are relying on the common law duty – it is important for the organisation to be as clear as it reasonably can be about which information it regards as confidential, so that people are in no doubt; this makes it much easier to take action if information is disclosed which should not have been.

In the case of volunteers it is also well worth considering a confidentiality pledge, that reminds volunteers of their duty of confidentiality – both while they are with the organisation and after they have left – and describes what information the organisation regards as confidential. All volunteers should be asked to sign this pledge, agreeing to maintain confidentiality, before they are given access to confidential information.

**Responsibilities**

Regardless of whether Personal Data is being handled by employees or by volunteers, the organisation they are working for has the responsibility for Data Protection compliance, and for maintaining appropriate confidentiality. This means that there must be clear policies and procedures, and everyone must be made aware of those that apply to them.

The organisation must ensure that the policies and procedures are brought to the attention of new volunteers in just the same way as they are brought to the attention of employees. This is likely to require:

- Clear guidance, appropriate to the role the volunteers play.
- Induction for new volunteers that covers their Data Protection and Confidentiality responsibilities.
- Refresher training from time to time.
- Support in the form of a designated person to whom any questions or concerns can be referred if they cannot be resolved by the volunteer’s supervisor.
- A confidentiality pledge that volunteers sign before being given access to confidential information.

It is usually unhelpful to see volunteers as a completely separate category from employees and to leave all Data Protection considerations just to the staff directly responsible for involving the volunteers. Where they carry out work in conjunction with employees, volunteers should be following the same policies and procedures, and should be given the same support, as their paid colleagues. Those with overall responsibility for Data Protection – and in most organisations those responsible for HR – should therefore be closely involved.

Where volunteers work autonomously – for example in the running of a local branch – some additional consideration has to be given to determine who is responsible for what. This is because responsibility for compliance with the Data Protection Act in any situation is the “Data Controller”. In almost every case the Data Controller is the organisation, not an individual employee or volunteer.
The Data Controller must, however, be a distinct legal entity. A group of companies cannot be treated as a single Data Controller; each company in the group is a Data Controller in its own right. For example, a charity and its linked trading company – even if it is wholly owned by the charity – are two separate Data Controllers.

Where an organisation has local branches it is therefore necessary to establish whether they are autonomous legal entities or an integral part of the parent body. There can be no half-way house. Most voluntary organisations nowadays are clear about this – partly thanks to the requirements of the Charities Act 2006.

In a unified structure, where branches are not independent, the parent body carries full responsibility for actions taken at branch level. In this situation the parent body must provide very clear guidance to branch officers on how they should handle Personal Data relating to members and others involved in branch activities. They should be asked to undergo the same type (if not the same degree) of induction and training as other volunteers, and they should sign a confidentiality pledge. The parent body should also reserve the right to audit their data handling, either at random or in response to a specific concern.

Where the organisation has a federal structure, with autonomous branches, the branch officers must be made aware that the branch carries full Data Protection responsibility, and is potentially liable for compensation payments or penalties from the Information Commissioner in the event of a breach. The parent body may, of course, wish to give guidance and support to branches in fulfilling their Data Protection responsibilities.

**Security (Seventh Data Protection Principle)**

Probably the most important of the eight Data Protection Principles – and certainly the one that gets the most attention – is the seventh. This says:

> 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.

Each organisation will have its own range of policies and procedures to cover these issues. Depending on the organisation they may cover issues such as:

- Office security: access control, visitor procedures, lockable storage, clear desk policy...
- IT security (data at rest): perimeter defences (firewall, anti-virus, etc), log-on credentials for the system itself and for key applications, backup procedures ...
- IT security (data in transit): password protection and encryption for files or devices that leave the office physically or by e-mail, procedures for ensuring that e-mails do not get sent to the wrong people, procedures for working remotely/from home ...
- Website security: protection against user details being stolen, protection against the site being damaged maliciously ...
- Non-electronic data in transit: procedures for sending confidential information by post, guidance on taking files out of the office ...
- Personnel: CRB checks, taking up references, supervision, monitoring ...
This is not the place to go into detail about what these policies and procedures should look like. The key point here is to recognise that volunteers are a significant point of weakness. They may, indeed, be less familiar than employees with the organisation’s professional working practice, and therefore pose a greater risk.

Volunteers should therefore receive specific training, not just to point out the existence of policies, procedures and guidance that they are expected to follow, but also to remind them of the many ways in which confidentiality can inadvertently be compromised. For example, they should be warned against:

- Discussing confidential information with partners and friends outside the organisation.
- Talking about confidential information in public places, either face to face or on the phone.
- Working on confidential material in public – on the train for example.
- Giving out information over the phone unless they are sure of the identity of the person they are speaking to and their authorisation to have the information.
- Sharing or disclosing computer access details (including through home computer systems that remember usernames and passwords).
- Losing confidential documents, or leaving them in places where they can be seen by unauthorised people.
- Sharing information about people who have not given permission for it to be shared (unless they know specifically that the sharing is permitted).
- Disposing of information carelessly when they no longer need it (e.g. failing to shred confidential documents).

Data quality (Third and fourth Data Protection Principles)

Volunteers may be responsible for data quality in a number of situations. They may:

- Assist with data entry in the office
- Prepare reports on home visits to beneficiaries
- Manage the membership records of a local branch
- Organise fundraising events that involve collecting data on donors

The third and fourth Data Protection Principles say that:

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

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

As with security, volunteers may not have the same professional expertise as employees, and may therefore need specific guidance on issues such as:

- What information to collect, and in what format
- How to design data collection forms
- How to ensure that the information they record is as neutral and accurate as possible
- How to keep information up to date – including how and when to offer people the chance to check that the information held about them is correct
It is often useful to remind people that individuals have the right of access to pretty much all of the information an organisation holds about them. A good test is therefore to imagine having to justify to the individual concerned the information that is held about them.

**Transparency, choice and limited purposes (First and second Data Protection Principles)**

Volunteers who are involved in obtaining information from people – especially on their first contact with the organisation – may need guidance on how to ensure that people know enough about what their data is used for and can exercise any choices on offer.

The operation of the first and second Data Protection Principles is complex, because of the reference in the first Principle to the “conditions in Schedule 2”. For the full text of the Schedule 2 conditions, see Appendix A. The Principles say, in effect:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed [without a legitimate reason].
- 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.

In many organisations volunteers will be expected to use materials prepared by professional staff. This should be encouraged in order to promote consistency over the information that people are given and the choices they are offered.

Where volunteers are responsible for creating their own data capture materials, they should be reminded that they must conform to any commitments made in the organisation’s Confidentiality policy or privacy statements. It may also be worth drawing their attention to the Information Commissioner’s Privacy Notices Code of Practice¹ which gives useful background to the legal requirements and helpful examples of good and bad practice in how to present information and options.

**Data retention (Fifth Data Protection Principle)**

There are no fixed rules about how long information should be retained. The fifth Principle says merely that:

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

Volunteers should be reminded that when they are acting on behalf of an organisation, the data they collect or hold belongs to the organisation, not to them personally. It should therefore be retained in accordance with the organisation’s retention schedule.

---

A retention schedule need not be complex; broad brush retention periods are usually acceptable, as long as they can be justified. For example, once information is no longer current it may perhaps be divided into ‘short-term’ – retain for months until a convenient time for disposal; ‘medium-term’ – retain for six or seven years, generally because it might be required for legal reasons; and ‘long-term’ – retain almost indefinitely, perhaps for historical or potential research purposes. In certain cases longer or shorter retention periods may be required by law or for other reasons.

When a volunteer stops being involved with the organisation, or steps down from a role, they should not retain any confidential information relating to the organisation or their role, but should consult the organisation about whether they are to destroy the information or return it for archiving.

**Data Subject rights (Sixth Data Protection Principle)**

Under the Data Protection Act, individuals have a number of rights. These include:

- The right of Subject Access (i.e. to have a copy of the data held about them)
- The right to opt not to receive direct marketing
- The right to prevent processing that causes them serious harm
- ... and various others

The sixth Principle states, simply:

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

In most cases volunteers should be advised not to attempt to handle instances where an individual wants to exercise their rights, but to refer all cases to the responsible person within the organisation. Many of these cases arise out of disputes or serious dissatisfaction, and they can involve delicate considerations. It is usually wise to ensure that they are handled only by an authorised senior person who is in a position to take legal advice if necessary.

The same approach should be taken in cases where an unusual – often official – request is made for data to be disclosed in breach of confidentiality, or where there is an indication that data should be disclosed to the appropriate authorities because of a concern about illegal or otherwise inappropriate behaviour. Volunteers should be advised always to refer the matter to the authorised person within the organisation, not to take precipitate action on their own behalf (except, of course, in situations covered by whistle-blowing provisions).

**Transfers abroad (eighth Data Protection Principle)**

Although relatively few UK voluntary organisations actually operate abroad, there are many opportunities to transfer information abroad, knowingly or inadvertently. These include:

- Publishing information on a website that is designed to be accessible throughout the world
- Making use of cloud computing services (or online applications such as Dropbox or SurveyMonkey) if the location of the data storage is not specified
It is probably difficult to restrict volunteers from taking advantage of these facilities, but the organisation may wish to provide guidance, either on how to proceed with caution or how to avoid putting Personal Data at unnecessary risk.

**Holding information about volunteers**

Most of the discussion above has focused on situations where volunteers are responsible for what happens to information about other people. Data Protection also applies, of course, to the information an organisation holds about volunteers, whether they are being recruited for your own organisation or by your organisation acting as a broker for others.

Running down the list of Data Protection Principles, this means:

**Data Protection Principle 1**

Do the volunteers know when they apply:

- which organisation is collecting their data?
- what it will be used for?
- whether it will be passed on to other organisations?

All of these things may be completely obvious but, if they are not, the volunteers need to be told – usually by including a statement on the form they have to complete.

**Data Protection Principle 2**

Have you been clear with volunteers about whether you will use their data for anything other than selecting and managing volunteers? For example, do you add volunteers to your fundraising database and send them appeals or invitations to events?

**Data Protection Principle 3**

Is there a good reason for all the information you collect about volunteers, both when they apply and then afterwards if they are successful?

Have you checked that your application forms do not ask for information that you would only need if the application is successful?

Is it clear which information applicants and/or successful volunteers must supply, and which is optional?

**Data Protection Principle 4**

How do you ensure that data is accurate (e.g. getting people to print or type their details, so that you don’t have to decipher handwriting)?

How often do you go back to your volunteers to check that their information is up to date?

Do they know who to tell if their details change?

**Data Protection Principle 5**

Do you have a clear policy on how long to retain information about applicants and volunteers? Remember that you have to justify why you need to keep the information.
There is no hard and fast rule, but you may want to think about:

- Applicants who have been turned down for a specific post and are not eligible for others: a month? three months?
- Applicants who have not been successful so far but may be considered in future: a year? – but they must be told that you will keep their details (and could ask for them not to be kept)
- Successful applicants: as long as they are working for you, plus a certain amount of time after they leave – perhaps a year or two while you are still able to give them a reference

There may be factors that affect this. For example, if your volunteers are working with vulnerable people there may be a requirement to keep certain information for much longer than the times suggested above.

**Data Protection Principle 6**
Do your volunteers know how to apply for access to their records?

**Data Protection Principle 7**
Are you clear who genuinely needs to see the information you hold about volunteers? Do you restrict access just to these people? Are you careful about the circumstances in which you would disclose or share information about your volunteers?

**Data Protection Principle 8**
If you store data in the cloud and it is not guaranteed to remain in Europe, are volunteers aware of this? Do you consult them before publishing their names or photographs on your website?

### Appendix A: Data Protection Principles and Schedule 2 Conditions

These are quoted from the Data Protection Act 1998, Schedule 1, Part I.

1. 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

   *the Schedule 2 conditions are that:

   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.

and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

[Schedule 3, as subsequently amended by Statutory Instrument, contains around 20 conditions, more restrictive than those in Schedule 2.]

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

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

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

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

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

7. 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.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.