

## Guidance Notes

# *Data Protection for Voluntary Organisations*

If your organisation handles personal information about individuals such as personnel records, details about service users, databases of donors, you will have a number of legal obligations to protect that information.

For voluntary organisations good data protection practice is important not only to comply with the law but also to build good trusting relationships with clients, volunteers, donors, etc.

All organisations in the UK, either businesses or voluntary, must comply with the Data Protection Act (1998), which came into force in March 2000. Under this Act, *it is an offence to release personal information without the person's consent*. This is being enforced by the Information Commissioner's Office.

The Data Protection Act is concerned with 'personal data', i.e. information about an individual (i.e. the data subject) that enables him/her to be identified, held on computer, or other electronic equipment and information held in a filing system or other record systems where information about an individual can be readily located. Personal data includes text as well as photographs, and video records.

Data protection does not apply to information about companies or organisations but it could apply to people named within the organisation.

**Some examples of personal data are:**

- Client or casework records
- Records of staff and volunteers
- Membership records
- Newsletter mailing lists
- Training and conference administration records
- Contact databases (with named individuals)
- Computer-based sales records
- Lists of consultants

Personal data and organisations holding personal data must comply with the **eight Data Protection Principles**.

**The eight Data Protection principles:**

1. Personal Data must be processed fairly and lawfully;
2. Be collected and used only for specified purposes;
3. Be adequate, relevant and not excessive in relation to the purposes for which it is collected;
4. Be accurate and up to date;
5. Be held no longer than necessary;
6. The rights of those you hold information about must be respected;
7. Be held securely with appropriate measures to prevent unauthorised access and use;
8. Special rules apply to transfer of data abroad.

**Some of the practical implications of these principles are:**

1. You should ensure that people about whom you hold data know that you hold that information and have given consent. You should give individuals the choice to agree or not to specific uses of their own personal information by including opt-out options.
2. You should inform people of the purposes for which you use the data and if you share that information with anyone else. If you share mailing lists with other organisations, check that their use of your mailing list is compatible with your organisation's purpose as specified.
3. You should inform people about whom you hold information, of the rights they have to know what information you hold about them and to place restrictions on the use and share of that information. You should stop using personal data within 21 days of an individual's request.
4. You should include a data protection statement in forms, leaflets, emails and/or website or place a notice in the office.
5. You should not continue to keep data without a good reason. If you keep information longer than what might be expected, then you need to inform the people about whom you are holding data. In most cases, no specific retention periods are given by law, however some type of records have statutory requirements, for example the statutory retention period for wage/salary records is 6 years. Ideally, your organisation should have a retention policy for personal data.
6. You should have in place security systems which are appropriate to the type of personal information you hold, in order to prevent unauthorised access to information as well as lost or damage of information. Destruction of data is also covered by the Data protection Act principles and should be done in a secure way to ensure that the details are irrecoverable.
7. You should have a confidentiality and security policy in place and ensure your staff and volunteers know about it and implement the procedures.

### **People you hold data about have the following rights:**

- To know what information is being kept about them and for which purposes.
- To be given the option to opt out of direct and telephone marketing, which also includes promotional activities of charities.
- To prevent the use of information if this is likely to cause them harm.
- To see any information held about them; requests need to be answered within a maximum of 40 days for a maximum fee of £10.
- To request the Information Commissioner to make an assessment of whether an organisation or individual is complying with the Act.

- Organisations or individuals who hold and use personal data might be required to notify the Information Commissioner by registering and paying a registration fee.
- Manually held data is exempt of notification, as well as membership records of non-profit organisations.
- Even if your organisation is exempt from notification you still need to comply with the eight data protection principles of good practice.
- To find out if your organisation needs to notify the Commissioner, check the 'on-line self assessment' in [www.ico.gov.uk](http://www.ico.gov.uk) or call 0845 630 6060 or 016 2554 5745.

### **E-mail and Web based information:**

- E-mail addresses are considered personal data under the Data Protection when they are specific to a person. You should take care in not disclosing them inadvertently.
- You should ensure that your organisation respects transparency and confidentiality in the use and distribution of e-mails.
- You should use a confidentiality disclaimer when sending organisation's e-mails and measures to improve the confidentiality of e-mails when necessary.
- You should ensure that your website provides the necessary information, when collecting personal data online.
- You should seek consent when publishing personal data (including photographs) on your website.

### **It is also important to note that ...**

- ✓ Staff and volunteers who access personal data should be properly briefed and trained on their responsibilities in relation to data protection.
- ✓ The management committee also needs to be aware of their responsibilities in relation to data protection, as they have the ultimate responsibility in terms of compliance with data protection.

## What do you need to do?

1. Make sure all your staff understand and follow the eight data protection principles.
2. Find out whether you need to notify the Commissioner about the personal information you process. Check the 'on-line self assessment' in [www.ico.gov.uk](http://www.ico.gov.uk) or call 0845 630 6060 or 01625 545 745.
3. Ensure that you get explicit consent from individuals to collect and use their personal information. For example, ask individuals to 'opt-in' by ticking a box after a statement explaining how the data will be used and by whom and requesting the form to be signed. Also include in all email marketing communications an opt-in consent from individuals before they are sent out.
4. Implement systems to keep personal information secure, such as disposing of confidential information securely by shredding, locking computers while away, prevent virus attacks, securely storing hard copy personal information, keep back ups of information, sign visitors in and out.
5. Ensure that staff only collects necessary and relevant personal information.
6. Ensure that staff is aware that rarely, if ever, should information on individuals be given in response to a telephone request.
7. Ensure your staff knows that people have a right to have a copy of the personal information you hold about them (however you may need to check the identity of the requester).
8. Keep personal information up-dated and relevant and dispose safely of information not needed any longer.
9. Inform staff and volunteers about any work place monitoring in operation, such as telephones or email.
10. Consider appointing a person within your organisation who will have an overview and take responsibility of checking data protection issues and practice within the organisation, by appointing a Data Protection Officer, preferable someone with authority within the organisation.
11. Undertake regular audits of current practice across the organisation checking as to whether it complies with the Data Protection Act. The findings of the audit can become the basis of your Data Protection policy.

If you require an example of an internal data protection audit or a Data Protection model policy, please contact Cristina dos Santos on 020 8875 2844, or email [smallgroups@wvsda.org.uk](mailto:smallgroups@wvsda.org.uk).

If you would like further information or advice on any of the issues in this Guidance Notes, contact the Wandsworth Voluntary Sector Development Agency (WVSDA) on 020 8875 2844/5/6 or Email: [smallgroups@wvsda.org.uk](mailto:smallgroups@wvsda.org.uk), [info@wvsda.org.uk](mailto:info@wvsda.org.uk)

More Guidance Notes can be found on our website, [www.wvsda.org.uk](http://www.wvsda.org.uk).

The Wandsworth Voluntary Sector Development Agency (WVSDA) provides information, advice and training to assist voluntary and community groups with issues relating to setting up and managing effective organisations. Whilst every effort is taken to ensure the information, advice and support we offer is current, relevant and accurate, it does not constitute legal advice.