



**Halton & St Helens**  
Voluntary and Community Action

# **Halton and St Helens Voluntary and Community Action (VCA) Data Protection Policy**

## **Introduction**

The Data Protection Act 1998 came into force on 1 March 2000. This policy sets out the rights and responsibilities of all staff at VCA who process personal data. This is important because the Act has an impact on everyone at VCA and the penalties for non-compliance can be fines or other forms of punishment under the law, either as an organisation or as individuals.

The policy covers all employees, volunteers, temporary staff, consultants and trustees.

The term “data processing” is very widely defined in the Act and includes obtaining, recording, organising, using, disclosing, deleting, and even simply holding data (information). Therefore, anything you do with information will amount to processing.

The term “personal data” is data that relates to a living individual who can be identified from that data and any other information that is in (or is likely to come into) the possession of the data controller.

There is a sub-category of personal data which is referred to in the Act as “sensitive personal data” and there are even more obligations on those who process this data. Sensitive personal data is information that relates to an individual’s political opinions, racial or ethnic origins, mental or physical health, sexual life, religious persuasion, trade union affiliation or criminal record.

The Act covers data held both manually and on computer.

## **Obligations and responsibilities**

### **The Eight Data Protection Principles**

Under the Act, all users of personal data must comply with 8 data protection principles:

1. **Personal data must be processed fairly and lawfully.** This means that data must be obtained in a way that is open, with an explanation of the purpose for which the data is to be used. In the case of sensitive data, it cannot be processed lawfully unless the subject of the data has given their consent.
2. **Data should be obtained only for one or more stated and lawful purposes and must not be processed in any way that is incompatible with those purposes.**

3. **Data must be adequate, relevant and not excessive in relation to the purposes for which it is processed.**
4. **Data should be accurate and, where necessary, up to date.**
5. **Data will not be kept for longer than is necessary for the purposes for which it is processed.**
6. **Data must be processed in accordance with the rights of data subjects.**
7. **Data must be protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.**
8. **Data must 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 data.**

### **Your Responsibilities**

All staff are required to maintain confidentiality in their work as appropriate. In relation to personal data it is essential to review procedures for handling such data to ensure that all processing is lawful under the Act. These points should be particularly considered:

- **Access** to personal data should be restricted to those who need it for clearly defined purposes. Personal data held on computer should be protected by regularly changed passwords, whilst data held in other ways should be kept secure when not in use. Failure to protect against unauthorised access would be an offence under the Act.
- Data must only be **used** for purposes for which it is collected. Data collected for one purpose must not be used for other purposes unless these were made known at the time the data was collected, or the data subject is advised and consents.
- Data should not be **held** for longer than necessary and so should be destroyed when no longer needed, or at the end of any statutory retention period. Only keep data if there is a good reason for doing so – getting rid of unnecessary data can also save on space.
- Take care when **revealing** personal data to anyone other than the individuals themselves. Where necessary, obtain evidence of identity and establish why the data is needed. Consider whether or not revealing the data is in accordance with the Act, and if in doubt, seek advice from a manager. The consent of the data subject should be obtained whenever possible.

## **Rights of Access to Information**

### **1. Employees**

Employees of VCA have the right to access information held on them by VCA. To do so, you should make a written request to the Chief Executive Officers PA, setting out in detail the information you wish to see. VCA has a right to charge for this access and staff will be charged £10 per request.

Information will be supplied within 40 days of the written request being received. Access to the information will be in the presence of a nominated person. The sole purpose of this is to ensure that no material is inappropriately removed or destroyed, and to protect the individual seeking access from any such allegations at a later date. You may, within reason, request one copy of any or all of the information to which you seek access. A record will be made of any copies requested and provided, including date and place, together with the name of the person providing them.

Access to references received will only be provided if the provider of the reference has consented and there is no other substantial reason for VCA to do otherwise.

Employees may challenge the accuracy of an entry made in the records and the data controller must respond to this challenge by investigating it and making any changes as necessary.

DBS disclosures and other information concerning members of staff will be kept in line with this Policy.

### **2. Service Users**

All service users have a right to access their files in the same way as employees. However, care must be taken to ensure that any documents that cannot be shown to the individual under the law remain confidential. Service users may challenge the accuracy of an entry as above.

### **3. Third Party requests for data**

Data must not on any account be disclosed over the telephone. The caller's identity will be difficult to verify. If you receive such a request you should ask the person to put the request in writing via letter, fax, e-mail, as appropriate.

Data can be disclosed to a third party without the consent of the data subject in the following circumstances only:

- Data required by law, eg data supplied to statutory bodies.
- Data that is in the vital interests of the data subject.
- Data that would prevent harm to a third party or self.
- Data that would prevent crime.
- Data that would be in the interest of national security.

A record must be kept on file of any disclosure, including date, to whom, and the reason for the request.

### **Exemptions to Access**

Access may not be permitted in the following circumstances:

- It would involve a disproportionate effort.
- The data subject has not provided sufficient information to enable the data controller to satisfactorily identify the data subject or otherwise comply with the request.
- The data controller has already complied with the same or a similar request within a reasonable period.
- Disclosure of the data would also disclose information relating to another individual unless:
  - the other individual has consented; or
  - it is reasonable to disclose the information without such consent.

Careful consideration should be given to what is “reasonable”, in relation to the last point, thinking through any duty of confidentiality owed to the other individual, any steps that the data controller might take to seek consent from them, and whether the other individual is capable of consenting.

### **Retention of Records**

The Data Protection Act states that data should not be kept for longer than is necessary for the purposes for which it is processed. Therefore, VCA sets out the following guidelines for retaining data. These guidelines relate to all employees at the VCA who may hold information about individuals.

- Applicants for jobs who are not shortlisted for interview: 6 months
- Applicants shortlisted for interview who are not successful: 12 months
- Ex-employees: 6 years
- Summary of record of service of ex-employees: 10 years
- Files on ex-service users should be kept for no longer than 7 years.
- All ERDF records shall be retained until 3 years beyond the closure of the programme or until 31<sup>st</sup> December 2025 whichever is the later.

This policy will be updated as necessary when new legislation on data protection is introduced.

VCA aims to provide its members, organisations and individuals with the best possible service.

However, we recognise that from time to time there may be occasions when users of our services feel that the quality or level of service provided falls short of what they could reasonably expect.

The goodwill and support of all members and other contacts is valued and if therefore you have a complaint to make, we would like you to tell us about it.

This is what you should do: -

1. The complaint should be made in person, by telephone, in writing, by email or via VCA Comments, Complaints and Compliments Leaflet to the Chief Executive Officer who will acknowledge in writing within 7 working days of the receipt of any complaint.
2. The Chief Executive Officer shall undertake to investigate the circumstances leading to the complaint.
3. The Chief Executive Officer shall communicate the results of any investigation to the complainant within a reasonable time – usually 21 working days.
4. Should the complaint relate to the Chief Executive Officer, the complaint should be made directly to the Chair or Vice-Chair of the Board of Directors who will investigate the circumstances and communicate the results of the investigation within a reasonable time – normally 21 working days.
5. The complainant shall have the right – if dissatisfied with the results of the inquiry – to put his/her case personally to the Board of Directors.
6. The Board of Directors shall be regularly informed by the Chief Executive Officer, of the number and nature of any complaints and the outcome.
7. Where appropriate VCA shall make a written apology (signed by the Chair of the Board of Directors) to the complainant.

### **Office Procedure**

Example of a Data Protection form (Appendix 1) which may be used routinely whenever data is collected from individuals.

**CONFIDENTIALITY**

**Appendix 1**

**Data Protection Consent Form**

**Data Protection Act 1998**

Under the Data Protection Act 1998 we, Halton & St Helens VCA, are obliged to obtain your consent if we want to store or process certain types of information about you. We cannot process your application or adequately identify vacancies for you without storing and processing this kind of information, so please read the following paragraphs and sign below to indicate your consent.

The information you give us either on your application form or subsequently will be stored and processed whether or not we succeed in finding an organisation or placement to refer you to.

Sensitive information, eg information about gender, disability and ethnic origin, will only be used for VCA staff and volunteers for the purposes of equal opportunities monitoring, and it will not be accessible to organisations or people outside VCA. If you have worked for us we will store data relating to you for up to 10 years. After that any information that is capable of identifying you will be destroyed.

We may process data relating to you for the purposes of statistical monitoring, strategic planning, publicity, fund raising or campaigning and we may disclose statistics derived from data relating to you to other bodies in connection with any of these purposes, but we will keep strictly confidential your name and address and any other details which identify you unless we have your express permission to disclose them.

**Please sign below to confirm that you have read this information and consent to our use of any information you give us for the purposes we have specified.**

We may contact you to advise you of new opportunities and other things we are doing. If you do not wish to be contacted or included in any mailing list please tick.

Signature: ..... Date: .....