Data Protection Policy and Procedures

This policy is available in other formats and languages upon request.

Date Policy Approved by Board	March 2014
Review Date	March 2016
SHR Regulatory Guiding Standards	GS1.2 Policies and procedures: We have high-quality written policies and procedures to guide our actions.
National Care Standards	Standard 10: You keep your rights as an individual.

Policy Statement

Viewpoint collects and uses information about customers, employees, volunteers and trustees. The collection and use of personal information is regulated under the Data Protection Act (1998). The Act applies whether the data is collected, managed and stored on paper, on computer or by any other method including CCTV. Viewpoint regards the safe management of personal information as an integral part of its function as an employer and service provider. As a registered data controller Viewpoint is legally obliged to adhere to the Data Protection Act (1998). The board and directorate are ultimately responsible for implementation of the policy.

Purpose & Scope

The purpose of this policy is to ensure that staff, volunteers and trustees are clear about the rights and principles of Data Protection, to ensure that there are guidelines in place and that these guidelines are consistently followed. Failure to adhere to the principles of the Data Protection Act (1998) is unlawful and could result in legal action being taken against Viewpoint or its' staff, volunteers or trustees. This policy extends to all staff, volunteers and trustees who may collect or process data on behalf of Viewpoint.

Principles

The Data Protection Act (1998) regulates the control and processing of information relating to living, identifiable individuals (data subjects). Data users must comply with the principles of good practice which underpin the Act. The eight principles of good practice are:

1. Personal data will be processed fairly and lawfully
2. Data will only be collected and used for specific purposes
3. Data will be adequate, relevant and not excessive
4. Data will be accurate and up to date
5. Data will not be held any longer than necessary
6. Data subjects rights will be respected
7. Data will be protected from unauthorised access, accidental loss or damage.
8. Data will not be transferred to a country outside the EEC, unless that country has equivalent levels of protection for personal data.

These principles apply to all personal data, whether held on computer, in manual filing systems or any other form of communication media. All Viewpoint employees, volunteers and trustees who process or use any

personal information in the course of their duties will ensure that these principles are followed at all times.

Confidentiality

During their work with Viewpoint, staff and volunteers will be dealing with personal information on a daily basis. They may also be told or overhear very sensitive information in the course of their duties. As well as adhering to their professional codes of conduct all must be aware that the Data Protection Act (1998) is very specific about how this information should be handled. In short, to comply with the law personal information must be kept securely and not disclosed to any unauthorised person. Staff paid or unpaid must abide by this policy.

Compliance

Viewpoint will regard any unlawful breach of any provision of the Act, by any staff, paid or unpaid, as a serious matter, which will result in disciplinary action being taken under our disciplinary procedures. Any such breach could lead to dismissal and criminal prosecution.

Procedures

The following procedures have been developed to ensure that Viewpoint meets its' responsibilities in terms of data protection.
For the purposes of these procedures personal data collected, stored and used by Viewpoint falls into 2 broad categories

1. Internal data/records – staff, volunteers, trustees
2. External data/records – customers, clients, members

1. Internal Data/Records

Purposes

Viewpoint obtains personal data (names, addresses, telephone numbers etc) on application forms, references and in some cases other documents, from staff, volunteers and trustees. This data is stored and processed for the following purposes:

- ✓ Recruitment
- ✓ Equal opportunities monitoring
- ✓ Volunteering
- ✓ Payroll
- ✓ To distribute organisational material e.g. meeting papers

Access

Personal contact details will only be made available to other staff or departments if it is a necessary part of their role e.g. line manager, payroll, HR. Any other information supplied on application forms e.g. qualifications, equal opportunities information, will be kept in secure filing cabinets and will not be accessed as part of the day to day running of the organisation.

Personal contact details will not be passed on to anyone outside the organisation without the explicit consent of the individual data owner, unless there is a legal duty of disclosure under some other legislation or statutory body code e.g. Care Inspectorate, HMRC.

A copy of staff, volunteer and trustee emergency contact details will be kept in the emergency file for health and safety purposes to be used in emergency situations only – fire, bomb threat, etc.

Staff, volunteers and trustees will be supplied with a copy of their own personal data, within 40 days, if a request is made. Viewpoint reserves

the right to charge for the administrative costs incurred in providing printed copies of personal data.

Accuracy

Viewpoint will take reasonable steps to keep personal data up to date and accurate. Individuals have the right to ask for inaccuracies in their personal data to be corrected. Personal data will be stored for 6 years after an employee, volunteer or trustee has left the organisation unless an individual specifically asks for their data to be destroyed beforehand. If no request is received, the data will be confidentially destroyed 6 years after the last entry.

Disclosure Scotland/PVG Information

Viewpoint will act in accordance with Disclosure Scotlands' code of practice.

Disclosures/PVG certificates will be kept for no longer than is necessary to complete the recruitment process and in any case no longer than 6 months, unless there is a dispute about the content.

Storage

Personal data is kept in both paper-based systems and on a password protected computer system. Every effort is made to ensure these systems are organised and secure. Please refer to Finance and ICT policies for specific guidance. Departmental managers have overall responsibility for the safe and secure storage of any personal data held in their departments. Viewpoint operates a "clear desk" policy at all times i.e. no paper files or computers containing personal data may be left open, accessible and/or unattended on the desk top.

Use of Photographs

Where practicable Viewpoint will seek consent from individuals before displaying photographs in which they appear. If this is not possible, for example a large group photograph, we will remove any photograph if a complaint is received. This policy also applies to photographs published on our website or in Newsletters

2. External Data/Records

Viewpoint obtains personal data from members, customers and clients. This data is obtained, stored and processed solely to assist staff and volunteers in the efficient running of services. The information is stored securely in both paper-based and computer systems. The data is stored and processed only for the purposes outlined in the agreement and service specification signed by the client, customer or member.

Consent

Personal data will not be passed on to anyone outside the organisation without explicit consent from the individual, unless there is a legal duty of disclosure under some other legislation or statutory body code e.g. Legal Power of Attorney, Guardianship Order, Care Inspectorate, HMRC, Police.

Accuracy

Viewpoint will take reasonable care to keep personal data up to date and accurate. Individuals have the right to ask for inaccuracies in their personal data to be corrected. Personal data will be stored for as long as the individual, customer or client uses our services. Where an individual ceases to use our services the data will be destroyed according to the schedule at appendix A.

Access

A large number of Viewpoint staff and volunteers will have access to personal data about customers and clients as part of their duties. All staff and volunteers are made aware of the Data Protection Policy and their obligation not to disclose personal data to unauthorised persons, during corporate induction training.
Individuals will be provided with access to their own personal data within 40 days of a formal request being made. Viewpoint reserves the right to charge for the administrative costs incurred in providing printed copies of personal data.
The Access to Health Records Act (1990) has been repealed to the extent that it now only affects the health records of deceased patients and it only applies to patients' records created since 1st November 1991.
Family, friends or representatives will not be given access to your information without your permission. If you are unable to give permission, because of incapacity, we will only disclose personal data to persons who hold a legal authority to act on your behalf – Appointee, Power of Attorney, Guardianship Order etc.

Storage

Personal data is kept in both paper-based systems and on a password protected computer system. Every effort is made to ensure these systems are organised and secure. Departmental managers have overall responsibility for the safe and secure storage of any personal data held in their departments.

Use of Photographs

Where practicable Viewpoint will seek consent from individuals before displaying photographs in which they appear. If this is not possible, for example a large group photograph, we will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisations website or in Newsletters.

Appendix A

Unless there is a dispute about a particular record the usual confidential destruction of personal/medical data will take place as follows:

Psychiatric records	20 years after the last contact or 3 years after death
Oncology records	20 years after the last contact or 3 years after death
All other records	6 years after last entry or 3 years after death
GP records	For the patients lifetime and 3 years after death
Other Personal information	6 years after last entry or 3 years after death
Personal Financial records	7 years after last entry or 3 years after death