Herts Vision Loss

Data Protection and Access to Information Policy

Reviewed June 2016

1. Introduction

This policy covers data obtained and retained by Herts Vision Loss (HVL) that relates to individuals, clients, volunteers or staff, who can be identified from that data. Both manual (paper based) and computerised records are encompassed within the scope of this policy.

The purpose of this policy is to ensure that: -

- Officers are clear about their responsibilities;
- Individuals are clear about their rights and responsibilities;
- Processes are in place to comply with UK and EU Data Protection legal requirements and law.
- All required permissions are gained and best practice is followed for the processing and storage of data.

HVL is a nominated data controller under the terms of the Data Protection Act 1998 and will discharge its responsibilities as such by enforcing this policy. As such, it must continue to be recorded on the Information Commissioners register and notify any changes.

2. Legal Requirements

Data Protection Act 1998

The Data Protection Act of 1998 regulates the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

All individuals involved in the processing of personal data must comply with the requirements of the Data Protection Act and with this policy and procedure.

EU Data Protection Regulation 2016

This Regulation, agreed in December 2015 and formally adopted in Spring 2016, is a new European data privacy framework, which includes the new EU data protection regulation. It requires organisations to secure personal data and introduces a tougher and more complex protection requirement. Encryption is recognised as the best way to comply with the requirements.

The new Data Protection Regulation will apply one consistent set of requirements for all organisations that hold data on European citizens. The legislation is very broad and

covers many aspects of personal data. EU countries have up to two years to implement the new requirements.

The Regulation applies to organisations within the EU and to those organisations outside of the EU that offer goods and services to, or monitor the behaviour of EU citizens. In terms of personal data security, this means implementing appropriate security measures to protect the data.
A more regular external Audit requirement will be instigated as a result of this regulation, which HVL must comply with.

Major data breaches put clients and individuals at risk of identity theft and financial loss, and businesses at risk of losing client loyalty, as well as regulatory fines.

Failure to comply may result in: -

- Action being taken by the Data Protection Information Commissioner against Herts Charity for the Blind, in the form of fines up to 4% of annual turnover.
- Criminal charges being made against the individual responsible for the breach that may be punishable by a fine or imprisonment.
- Disciplinary action being taken by HVL against the employee responsible.

The Act extends to information retained on, clients, volunteers, contractors, consultants, etc., as well as all HVL employees.

The actions which HVL must take to comply with current and new legislations are:

- Get privacy policies, procedures and documentation in order and keep them up to date
- Form a governance group that oversees all HVL privacy activities, led by a senior manager or executive. The group should develop metrics to measure the status of privacy efforts, report regularly and create statements of compliance.
- Implement a breach notification process and enhance your incident management processes and your detection and response capabilities.
- Any data breach must be notified to the relevant data protection authority, even if protective measures, such as encryption, are in place; or the likelihood of harm is low.
- Prepare HVL to fulfill the "right to be forgotten", "right to erasure" and the "right to data portability". A strategy covering topics such as data classification, retention, collection, destruction, storage and search.
- Create and enforce privacy throughout HVL systems' lifecycles to meet the "privacy by design" requirement. Ensure privacy controls are stronger, simpler to

implement, harder to by-pass and totally embedded in a system's core functionality.

3. Herts Vision Loss Policy and Procedure

3.1. Principles

3.1.1. General

HVL is committed to ensuring it complies with the law and best practice principles regarding the retention and processing of personal data. At all times personal data held on computer or in manual filing systems under HVL's control will be:-

- Processed fairly and lawfully ;
- Obtained only for specific and lawful purposes, and will not be used in a manner which is incompatible with these purposes;
- Adequate, relevant, and not excessive for the purposes for which it is processed;
- Processed in accordance with the individual's rights;
- Accurate and kept up to date
- Kept secure
- Data will not be kept any longer than necessary
- Data will not be transferred to recipients/countries without adequate privacy protection.
- 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.

3.1.2. Personal data

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- That data
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

3.1.3. Sensitive data

Where HVL requires to process sensitive information, as defined by the Act, then we will obtain the individual's consent by appropriate means. During the process of gaining this

consent we will provide information covering the specific detail of the processing of the data including the purpose for which it is required.

Sensitive data is defined as personal data consisting of information as to:-

- Racial and ethnic origins,
- Physical and health condition
- Political opinion
- Religious or other beliefs
- Trade union membership
- Sexual orientation
- Criminal proceedings or convictions

3.1.4. HVL Values

In line with our values of Honesty and Respect we will adopt the principle of openness with individuals regarding data recorded on them whilst maintaining appropriate confidentiality on their behalf.

To comply with Data Protection Act and requirements in practise, HVL must:

a. Have legitimate grounds for collecting and using the personal data;
b. Not use the data in ways that have unjustified adverse effects on the individuals concerned;
c. Be transparent about how the data will be used, and give individuals appropriate privacy notices when collecting their personal data;
d. Handle people's personal data only in ways they would reasonably expect; and
e. Make sure nothing unlawful is done with the data.

3.2. Definitions

3.2.1. Data

The meaning of data for the purpose of this policy is:

- Any recorded information held in a relevant manual, call receiving staff or computerised filing system (including e-mail and Internet) that relates to an individual who can be identified from the data.
- This includes, but is not exclusive to, personal records retained in Human Resource and Payroll departments, and by Services. Similar or equivalent records retained elsewhere are also included under the Act.
- Data encompasses both facts and opinions about the individual.

3.2.1. Processing

Processing means obtaining, recording or holding data or carrying out any operation on data. This will include almost all activities involving data.

3.2.3. Computer or manual filing systems

Computer or manual filing systems means any set of information relating to individuals that is structured, either by reference to individuals or criteria, in such a way that specific information relating to an individual is readily accessible.

There are from time to time requirements to establish one off records for particular purposes, e.g. complex disciplinary cases, grievance etc. where a secondary record may be established. These need to be referenced in the main record and the same rights and responsibilities apply.

3.2.4. Accurate Data

Accurate data means that:-

- Where the information is factual, it is correct;
- Where the data is an expression of opinion, HVL believes that it is fair and based on factual evidence e.g. documented examples of an individual's behaviour, diagnosed health conditions, competencies etc.

3.3. Procedure

3.3.1. Record Keeping

HVL will keep such records required to facilitate the efficient running of the business, (such as records relating to client list, employment, payroll, training, sickness absence, etc.) and to comply with relevant legislation e.g. tax and insurance obligations, Minimum Wage Act.

HVL will ensure that information is always recorded with due regard to fair treatment and privacy, by following these guidelines:-

- Ensure fair collection and use of personal information.
- Specify the purpose for which the information is used.
- Not recording any data classified as 'sensitive' without express permission, unless it is necessary to do so for one of the specific purposes allowed by the Act e.g. suspicion of criminal activity.
- Only holding information which is necessary for legitimate business purposes
- Not holding information which is excessive for these purposes or for longer than necessary
- Ensuring all information is accurate and up-to-date by correcting any errors of fact as soon as possible after we are advised of it.
- Apply checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard information.

- Ensure the rights of people about whom the information is held can be fully exercised – to be informed, have access to own information within 40 days, to prevent processing and ability to correct, rectify, block or erase information regarded as incorrect.

The information will be kept in a secure place and the relevant staff member is responsible for ensuring that security and appropriate confidentiality is maintained.
If HVL can demonstrate that personal data was subject to technological protection measures rendering it unintelligible to unauthorized people (e.g. encryption), notification affected data subjects of any breach is not required.
If you can show that the personal data was encrypted the likelihood of being fined as a result of a breach should be very greatly reduced.

3.3.2 Access to data
Access to personal data will be restricted to the individual to whom it relates and other people who have a legitimate business need to know.

HVL will not disclose any information about individuals to internal or external third parties unless it is lawful to do so, or where express consent has been given.

By law we are required to provide information if ordered by the Courts or requested as part of an official enquiry from organisations such as the:

- Department of Work and Pensions;
- Inland Revenue;
- HM Customs & Excise;
- Child Support Agency
- Police

3.3.3. Individual Rights and Responsibilities
Individuals have the right of access to their own data as retained in relevant computer or manual filing systems. To implement this right a written request to the Chief Executive Officer is required.

Individuals may, within reason, request one copy of the entire data if they wish.

Individuals may challenge the accuracy of an entry in the data and, where this is proved to be inaccurate to have this entry corrected or removed. They may also challenge the legitimacy of making or keeping particular data in the record.

This right of access only extends to data that is stored in such a way that it is readily retrievable by reference to the individual (e.g. by name, ID number). It does not apply to

a few particular types of data, e.g. employment references, which are exempt under the provisions of the Act.

Individuals have a responsibility to ensure that all source documents are completed accurately and truthfully. Source documents include application forms and related documentation, medical and other questionnaires, etc. that request the provision of data.

Individuals also have the responsibility of keeping their personal data up to date by advising the Charity of any relevant changes e.g. change of address.

3.3.4. Staff Responsibilities

Managers, or other employees involved in the processing of data are responsible for compliance with the terms of this policy in its entirety. In particular:

- Data should not be processed without giving consideration to the principles set out at the beginning of this policy.
- Where a written request is received requesting access to data it will be responded to in writing making suitable arrangements for access to take place within 28 working days of the request.
- The Chief Executive Officer will decide the most practicable access arrangements dependent upon the location of the individual making the request.
- The Chief Executive Officer will ensure that the access happens in the presence of a nominated person who will ensure that no material is removed or destroyed.
- Where the individual requests a copy of data the nominated person will record the copies requested and provided, including the date and place, together with the name of the person providing them.
- Where a challenge to the accuracy or legitimacy of data is received the Chief Executive Officer will consider the issue and make a decision in line with the principles of this policy. This decision, and reasons for it, will be communicated to the individual in writing within 21 days of the challenge being received.

HVL will ensure:

- A specific staff member responsible for data protection in the organisation
- Everyone, Staff and volunteers, handling personal information understand they are responsible for good data protection practice, and are fully aware of this policy.
- All personnel handling data information is appropriately trained and supervised to do so.
- Performance and methods of handling personal information are regularly assessed and evaluated
- Queries about data are promptly and courteously dealt with.
- Data sharing is only carried out under written consent.

- Data and other documents are kept in a secure environment.
- Data held electronically is protected by Passwords
- Individual passwords are not shared and not easily compromised.

3.3.5. Retention of data
In relation to client records; records will be retained for the appropriate period as defined by the act.
In relation to staff and volunteer records; these will be retained as defined by statutory regulations.
Data held by HVL will be regularly reviewed and culled as appropriate.
Compliance audits will be conducted annually or as directed by the Information commissioner.

4.1 Policy review
HVL will review this policy annually in accordance with EU regulation and the Data Protection Act.

5.1 Notification to the Information Commissioner
The Information Commissioner maintains a public register of data controllers. HVL is registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

The Chief Executive will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner within 28 days.

6.1. Relationship with existing policies and supporting documentation
This policy has been formulated within the context of the range of HVL policies.

In addition, pro formas in use for requesting consent to store data (from clients, staff and volunteers) are included in this framework.

Reviewer: Alex Hickinbotham
Date: 1.6.16