General Data Protection and Access Information Policy

General Data Protection and Access Information Policy

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 General Data Protection Regulations (2016) 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.

(Definitions

Processing of information – how information is held and managed.

Information Commissioner - formerly known as the Data Protection Commissioner.

Notification – formerly known as Registration.

Data Subject – used to denote an individual about whom data is held.

Data Controller – used to denote the entity with overall responsibility for data collection and management. HVL is the Data Controller for the purposes of the Act. **Data Processor** – an individual handling or processing data

Personal data – any information which enables a person to be identified

Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Charity)

2. Legal Requirements

The General Data Protection Regulations (GDPR) were introduced into UK law by the UK Government at the end of May 2018 to replace the 1998 Data Protection Act. These new regulations extend the rules for the way information about people is handled and to give legal rights to people who have information stored about them.

GDPR is a reaction to the increase in the amount of personal data that is collected and stored by organisations, including employers. As the amount of data collected in likely to increase it is important to consider the types of information kept and how it is accessed, processed, and stored.

This document defines the way HVL has responded to the GDPR and outlines the policies and procedures for ensuring compliance.

Data Protection Act 1998 regulated the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. This has now been replaced with the GDPR.

All individuals involved in the processing of personal data must comply with the requirements of GDPR 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 because 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 Vision Loss, in the form of fines up to 4% of annual turnover or 20 million Euros. This is the maximum fine that can be imposed for the most serious infringement, for example not having sufficient processes in place, when handling data or violating the core of Privacy by design concepts.

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.
- Ensure the Finance and Governance Committee that oversees all HVL privacy activities, led by a senior manager or executive develop metrics to measure the status of privacy efforts, report regularly and create statements of compliance.
- Implement a breach notification process and enhance our incident management processes and our 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 fulfil 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

Principles

HVL is committed to ensuring it complies with the law and best practice principles regarding the retention and processing of personal data. The lawful basis for processing is set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:

Consent – the individual has given clear consent for you to process their personal data for a specific purpose.

Contract – the processing is necessary for a contract that you have with the individual, or because they have asked you to take specific steps before entering the contact.

Legal Obligation – the processing is necessary for you to comply with the law **Vital interests** – the process is necessary to protect someone's life.

Public task- the processing is necessary for you to perform a task in the public interest or for your official functions and the task or function has a clear basis in law. **Legitimate interests** – the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data overrides those legitimate interests.

Source ICO – "Lawful Basis for Processing" https://ico.org.uk.for-

organisations/guide-to-the-general-data-protoection-regulation-gdpr/lawful-basis-for-processing/#ib3

Personal data
The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and special categories of 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.

Special categories of personal data.
Where HVL is required 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.

Special categories of personal data are defined as personal data consisting of information as to: -

- Racial and ethnic origins,
- Political opinion
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Health
- Sex life and Sexual orientation

If the data being processed falls in the special category data, then you must be able to demonstrate a lawful basis under article 6 and article 9 of the GDPR.

HVL Values
In line with our values, we will adopt the principle of openness with individuals regarding data recorded whilst maintaining appropriate confidentiality on their behalf.
To comply with GDPR 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.

4. Consent

HVL must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data cover information relating to:

- The racial or ethnic origin of the Data Subject.
- His/her political opinions.
- His/her religious beliefs or other beliefs of a similar nature.
- Whether he/she is a member of a trade union.
- His/her physical or mental health or condition.
- His/her sexual life.
- The commission or alleged commission by him/her of any offence
- Online identifiers such as an IP address
- Name and contact details
- Genetic and/or biometric data which can be used to identify an individual.

Special categories of personal information collected by HVL will, in the main, relate to service users' physical and mental health. Data is also collected on ethnicity and held confidentially for statistical purposes.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a rule HVL will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Services Manager or Chief Executive for advice.

4.1. Obtaining Consent

Consent may be obtained in several ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email.
- Face-to-face/written.

- Pro-forma should be used.

4.2. Telephone

Verbal consent should be sought and noted on the case record.

4.3. E-mail

The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of insurance products was to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record (e.g., ACT). The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age, then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by HVL then the staff member should discuss with the CEO at the earliest opportunity

5. Ensuring the Security of Personal Information

Unlawful disclosure of personal information

- It is an offence to disclose personal information ‘knowingly and recklessly’ to third parties.
- It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.
- Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need-to-know basis.
- A client’s individual consent to share information should always be checked before disclosing personal information to another agency.
- Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive should first be sought.
- Personal information should only be communicated within HVLs staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information

may not be overheard by people who should not have access to such information.

6. **Ethnic Monitoring**
   For HVL to monitor how well our staff, volunteers and service users reflect the diversity of the local community we request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a passworded database for statistical purposes.

7. **Use of Files, Books and Paper Records**
   In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal / and/or special categories of personal data at home or in your car, the same care needs to be taken.

8. **Disposal of Scrap Paper, Printing or Photocopying Overruns**
   Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

   If you are transferring papers from your home, or your client's home, to the office for shredding this should be done as soon as possible and not left in a car for a period. When transporting documents, they should be carried out of sight in the boot of your car.

9. **Computers**
   Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only. Computer monitors in the reception area, or other public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, you should lock your computer when leaving it unattended.

   Firewalls and virus protection to be always employed to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

   Documents should only be stored on the server or cloud-based systems and not on individual computers.

   Where computers or other mobile devices are taken for use off the premises the device must be password protected.

10. Cloud Computing

When commissioning cloud-based systems, HVL will satisfy themselves as to the compliance of data protection principles and robustness of the cloud-based providers.

11. Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement:

12. Herts Vision Loss Privacy Notice

This privacy notice explains how Herts Vision Loss (HVL) (the Data Controller) will use any personal information we collect about you when you use our services.

13. What information do we collect about you?

The information that HVL will collect varies depending on how you use our Services. We are using the information provided in this case because we have a legal obligation, this means we collect your personal information from you so that we can carry out a function that you have requested; provide a service we choose to provide or carry out processing where you have agreed to share the data with us. Each time you contact us we will make a note on your record.

14. How will we use the information about you?

We use the information to process your request, complaint or query and send you our Newsletter if requested. We will only share the information to enable us to deal with your request and we will let you know if we share your information with other agencies.

We will not share the personal information we hold with any external organisations unless agreed with you. We will always tell you who we will share the information with.

We will ensure that all personal information is kept securely.

15. How long will we keep this information? We will destroy this personal information in accordance with our Disposal Schedules, please see the General Data Protection Policy Document on the website. To determine how long we should keep information, we consider what the legislation states and what is good practice. This means we will securely destroy the information once we no longer need it. If you would like to know the specific period that relates to your personal information, please contact office@hertsvisionloss.org.uk

16. Individuals' Rights

You have a right to request a copy of the personal information that we hold about you. If you would like a copy of some, or all your information, please contact us on office@hertsvisionloss.org.uk and ask for a subject access request.

If you would like to be removed from our records, please contact us on 01707 324680 or email office@hertsvisionloss.org.uk

If you consider we hold inaccurate personal information about you, you can

contact us to ask for this information to be corrected. We will update our records within 30 days. Please contact us at office@hertsvisionloss.org.uk

17. Cookies

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to make your use of the internet better. For further information on how we use these and how you can control it, please visit http://www.hertsvisionloss.org.uk/

18. Changes to our Data Protection Policy

We have a Data Protection Policy in place, and this can be found here: HVL premises, 2 Brownfields, Welwyn Garden City.

This policy is reviewed bi-annually.

19. Data Protection Officer

Our Data Protection Officer for the purposes of the General Data Protection Regulation is The CEO, Clement Musonda and can be contacted by email: Clement.Musonda@hertsvisionloss.org.uk or call 01707 324680.

20. How to contact us

Please contact us if you have any questions about our Data Protection Policy, or concerns about how we handle your information: by emailing office @hertsvisionloss.org.uk or write to us at: Herts Vision Loss. 2 Brownfields, Welwyn Garden City, Herts AL7 1AN.

21. Complaints

You have a right to complain to the Information Commissioner if you are unhappy with how we process your personal information. You can do so through their website: https://ico.org.uk/concerns/ or by emailing: casework@ico.org.uk or calling their helpline on 0303 123 1113.

22. Personnel Records

The Regulations apply equally to volunteer and staff records. HVL may at times record special categories of personal data with the volunteer's consent or as part of a staff member's contract of employment.

For staff and volunteers who are regularly involved with vulnerable adults, it will be necessary for HVL staff to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Senior Management Team. If there is a positive disclosure the Chief Executive will discuss this, anonymously, with the Chair and our insurers to assess the risk of appointment. Trustees and insurers should not see the report itself.

23. Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g., documents and programmes related to work for HVL should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer, they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

When sending emails to outside organisations, e.g., social worker or hospital staff, care should be taken to ensure that any identifying data is removed and that codes (e.g., initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (e.g., clients care plan kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g., on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Enablers needing to take paperwork away from a client's home (e.g., unable to make a required phone call during the visit) must ensure that it is returned to the client's home on the next visit.

If you are carrying documents relating to a number of clients when on a series of home visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the client's home. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain HVLs contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

24. Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

- Client records – 6 years after ceasing to be a client.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.

Other documentation, e.g. clients care plan sent to a worker as briefing for a visit should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

Computerised records e.g. ACT to be anonymised 6 years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.)

25. What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Senior Management Team and/or Quality Assurance & Systems Manager, to prevent a reoccurrence. Action will be taken and outcomes to determine whether it needs to be reported to the Information Commissioner and for reporting to the Board of Trustees. There is a time limit for reporting breaches to ICO so the CEO should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

26. The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).

Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

Individuals have a right to have their data erased and to prevent processing in specific circumstances:

- Where data is no longer necessary in relation to the purpose for which it was originally collected
- When an individual withdraws consent
- When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- Personal data was unlawfully processed.

An individual has a right to restrict processing – where processing:

- Is restricted, HVL is permitted to store the personal data but not further process it. HVL can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

HVL will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (HVL) must comply with such requests within 30 days of receipt of the written request.

27. Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence.

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

28. Further Information

Further information is available at www.informationcommissioner.gov.uk

29. Details of the Information Commissioner

The Information Commissioner's office is at:
Wycliffe House
Water Lane
Wilmslow,
Cheshire SK9 5AF.

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

The condition detailed within this document may only be amended following discussion and approval of the Board of Trustees which in turn should be properly recorded.