HVA - 5 April 2018

Data Protection and Privacy Policy – the rationale

Introduction

The Herpes Viruses Association has a legal obligation to comply with the laws of data protection and data privacy. The GDPR applies in the UK (from 25/5/2018). The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. This policy seeks to establish the best practices for Trustees and to ensure the potential risks are known in order to mitigate against them occurring. On the date of production of this policy, an excerpt of the Data Protection Act 1998 is captured within this document. This policy should be subject to a periodic review.

The Data Protection Act

The **Data Protection** Act regulates the use of "personal data".

Data means information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

More key definitions are available from the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Data Retention

Purpose: Data should be collected for a specific purpose.

HVA will not collect data for one reason and then start using it for another.

- Members' data (name and contact details) are collected so that information can be sent out to subscribers.
- Shoppers' data (name and contact details) are collected so that purchasers can reorder without having to input contact details each time they order.
- Shingles enquiries' data (name and contact details) are collected for so that further information on the treatment etc. of shingles can be sent to them.

Storage: The data is stored safely, securely and in an organised way. HVA is mindful that individuals can request to see what data HVA holds on them so it should be easily accessible.

Length of retention: For overview of service provision and for statistical research, a minimum amount of data is kept securely.

People can request that they will not be contacted again. A minimum amount of information is retained for legal/financial reasons and to ensure their preference is respected.

Website

HVA operates a website that the public can view.

The only access that the public has to the website is on the shop page, where they can enter their details and credit/debit card information. The name, contact details and items required are sent to the HVA. Their credit/debit card information is processed by Stripe and the HVA does not see these.

Other donation tools are available on the website. These allow totally anonymous donations.

Website Security

Currently, the website is on a server hosted by Cloud Above. No financial details are obtained or stored on this server.

The HVA's website has an SSL Certificate.

Cookies

At the date of production of this policy, the website operated with implied consent to the use of cookies. This is stated on the website.

The cookies used on the HVA's site are minimal, non-invasive and are managed by third parties, predominately Google for the Google Analytics. This is something to be mindful of if HVA changes the way in which cookies are used in the future and it may be decided to change the approach to an explicit consent.

Website Related Data

On the date of production of this policy, there were no methods for the public to comment on the HVA website.

Membership

All information regarding membership is treated as private and confidential. Membership lists and data are stored securely as previously outlined. All email correspondence to members originates from official HVA email addresses – or MailChimp.

HVA ensures that personally identifiable information is not released or communicated to other members. MailChimp or the BCC line are used to send e-mailings to members.

Emails sent out to members are only for the purpose the data was collected for. The data is never sold, passed on to third parties or marketed to with unrelated products. All emails sent out are to those who have expressly opted in to receive such communications and compliant with the laws surrounding SPAM messages.

Subject Access Requests

Under the GDPR, an individual has the right to request a copy of all of the information that HVA store that is related to them. HVA may charge an administrative fee up to £10 and must respond within 40 calendar days in-line with the legal requirement.

Responsibility of Trustees

All trustees, staff and volunteers of the Herpes Viruses Association (HVA) have a responsibility to ensure that the data held by and on behalf of the charity is adequately protected. Any data that is not in the public domain should be subject to security measures to ensure it remains confidential. HVA may be liable for financial penalties if this is not implemented.

Sources of Vulnerability

Trustees, staff and volunteers are aware of both physical and digital data that can arise from a number of sources such as:

1. Correspondence (letters, emails, voicemails, text messages)
2. Membership lists
3. Financial information (reports, bank accounts and donation lists)
4. Trustee documentation (reports, proposals, trustee meeting notes/action lists/minutes)
5. Other relevant items

Trustees will need to be aware of ways in which data can become compromised, lost or shared in order to implement adequate measures to mitigate the risk of this occurring; and should be aware of the areas of concern and the best practice guidance.

Physical Documents

Main areas of concern: misplacing, losing or have them stolen.

HVA discourages the printing of documents unless absolutely necessary; particularly when these documents include identifiable or sensitive information about HVA members.

Documents are kept in a safe and secure location and are not left in view of others. The office is locked when not occupied by staff.

These documents are disposed of securely when there is no further need to hold them.

Electronic Data

Main areas of concern: misplacing, losing or having physical computer equipment stolen and not implementing sufficient security measures to adequately protect data.

The HVA has electronic data on the office computer regarding the charity and its service users which has to be safeguarded. [The security standards implemented on any computer equipment and the computers in which they use or access materials, data and information related to HVA must be sufficient.] In addition, all cloud-based services are subject to the same requirement. This includes all email accounts, web-based storage accounts and anything else where the data is not a sole copy physically stored on HVA's machine.

- Laptops and/or computers are physically locked in the office when it is not occupied.
- No HVA work is performed on laptops/computers off-site.
- The HVA's computers contains anti-virus software which is kept up-to-date and the computers are periodically scanned for virus and malware.
- All computers require a password.
- Passwords are changed periodically, twice a year.
- Passwords should meet a certain complexity criterion which:
  - o Use both upper- and lower-case letters (case sensitivity)
  - o Include one or more numerical digits
  - o Include one or more special characters, e.g. @, #, $ etc.
  - o Not use words found in a dictionary or the user's personal information
- Be mindful of the transfer of data.
- Backup, copies of data and removable media such as USB sticks or hard drives, will be suitably protected and/or encrypted. We will use passwords as outlined above.
- The HVA does not operate any tablets, mobile phones and other devices that are capable of accessing data related to HVA. Should these be used at a later date, they will be:
  - o Subject to the same security measures.
  - o Setup to request a passcode.
  - o Capable of being wiped remotely should it become compromised, lost or stolen.

Data Loss

The consequences of data loss can be as damaging as the consequences of data breaches. All criteria listed for breaches applies to the risk of loss. This is for both physical and non-physical data.

Reporting

The HVA knows that as soon as any trustee, staff member or volunteer becomes aware that a breach or data loss, or a potential breach or data loss has occurred, they have a responsibility to report this to the Board of Trustees without delay and as soon as practically possible. If a person is unsure whether a breach has occurred or not, it is advisable to err on the side of caution and report it.

HVA shall make all reasonable endeavours to act swiftly and without delay when a breach or potential breach is reported. Depending on the circumstances and nature of the reported breach, beyond any legal obligations upon HVA, it may be voluntarily reported to necessary parties which includes, but not limited to: Information Commissioner's Office, Charity Commission Office, Regulators, Solicitors, Lawyers or Law Enforcement entities.

Specialist Areas of Operation

Access to relevant information: trustees, staff and volunteers only have access to the data that they actually need.

Finance

Trustees and staff who are involved with the financial elements of HVA are responsible for ensuring that the security of HVA's financial records, bank accounts and associated data remain secure. Appropriate security is used when accessing web-based or telephone-based banking systems. The reports, financial information and details to access these accounts are treated as strictly confidential and only shared when absolutely necessary.

.

Additional Resources

Find more information from the Information Commissioner's Office website where there is a section specifically related to charities: https://ico.org.uk/for-organisations/charity/

https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/