Hart Voluntary Action Limited
Data Protection Policy
Incorporating GDPR

1. Introduction

1.1 Current data protection legislation permits Hart Voluntary Action Ltd (HVA) to process individual personal data, providing it is relevant to the carrying out of our business. However, from May 2018 new data protection regulations came into force which significantly enhanced UK data protection practices. The changes had implications for many of the aspects of the HVA's operations, including finance, IT, HR, and communications. They also impacted on how HVA deals with service users and external organisations. The regulations cover in much more specific detail than previous data protection legislation the areas of Awareness, Information Held, Communicating Privacy Information, Individuals' Rights, Subject Access Request, Legal Basis for Processing Personal data, Data Breaches, Data Protection Impact Assessments, Data Protection Officers, and International Implications.

1.2 The Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) work together to regulate how organisations handle personal data in the UK. The DPA 2018 supplements the UK GDPR and extends data protection laws to areas that the GDPR doesn't cover. It is enforced by the Information Commissioner's Office (ICO).

1.3 This policy sets out Hart Voluntary Action's approach to meeting the requirements and, more importantly, ensuring that all personal information is held securely and with the consent and support of all staff, volunteers and service users.

2. Personal Data

2.1 General Overview

2.1.1 HVA is under an obligation to protect the confidentiality of the information held and to ensure that personal data is not divulged to others unless in doing so it strictly follows the purpose for which the information was supplied.

2.1.2. HVA Trustees are the Data Controller, HVA staff and volunteers are Data Processors for the information held. HVA and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

2.1.3 All members of staff and volunteers who have access to personal information, gained via association with HVA, will be expected to read and comply with this policy.

2.2 Legitimate/Legal Interest

2.2.1 HVA may process personal information without an individual's knowledge or consent where:

- this is required or permitted by law and HVA needs to protect an individual's interests (or those of someone else) in an emergency
- HVA has a need to use such information in connection with a legal claim
- An individual has already made such information public, such as religious or philosophical beliefs or political opinions.

2.2.2 When processing personal information based on a legitimate interest, HVA will make sure that it is exercised proportionately and is always balanced against the privacy rights and other legal rights of the individual.

2.3 Who has responsibility for data protection in HVA?

- The Trustee Board have overall responsibility for compliance.
- The Chief Executive has day to day management responsibility.

- The Senior Administrator has responsibility for managing and processing staff data privacy, consents and processing.
- Individual staff have responsibility for any day to day personal information they may obtain and process.

2.4 Any enquiries about any aspect of HVA's data protection should be directed to the Data Controller, including general queries, specific personal staff questions, subject access requests and/or real or potential breaches of data or data protection requirements. Further information on their responsibilities is contained in paragraph 7.1 below.

2.5 Personal Data

- Shall be processed fairly, lawfully and in particular shall not be processed unless specific conditions are met.
- Shall be obtained only for one or more of the principles specified in the Data Protection Act and shall not be processed in any manner incompatible with that purpose.
- Shall be adequate, relevant and not excessive in relation to its purpose.
- Shall be accurate and where necessary kept up to date.
- Shall not be kept for longer than is necessary and within lawful legislation.
- Shall be processed in accordance with the rights of data subjects under the Act.
- Shall be kept secure by the HVA who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to personal information.
- Shall 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 personal information.

3. Privacy Notices and Consents

3.1 HVA will issue individual Privacy Notices to all new and existing staff, volunteers and service users. This will detail all the types of personal information which HVA holds and processes, its purposes, how it is processed, why and the security provisions.

3.2 The Notice will also detail how an individual can have access to their information should they wish to. Individuals have the right to amend inaccuracies, add or delete any information held. However, they will be reminded that the deletion of any information which is relevant to their employment, working with HVA, could have a detrimental effect on their employment, work with HVA.

3.3 The Notice will include the option for individuals to confirm their consent to HVA holding and processing their personal information. This consent will be held in their personal file.

3.3.1 HVA will have a copy of the HVA Privacy Notice on its website.

4. Training of staff

4.1 All staff are required to undertake training and/or briefing sessions on HVA's and their personal responsibilities under the data protection regulations. This will be covered in the induction training for new recruits.

5. Dealing with leavers' information

5.1 All personal information will be held for up to a period of six months. This is to facilitate any requests for references. However, individuals will be asked on leaving whether they consent to any or all of their personal information being held by HVA. They have the right to consent to some or all of

their information being deleted on leaving. They will be asked to review their Privacy Statement and confirm which information they wish retained or deleted.

5.2 All information will be securely shredded by at least six months or shorter if advised by the leaver after leaving HVA. However HVA has to keep financial information for 7 years from a legal standpoint

6. Dealing with recruitment information

6.1 Successful candidates will be dealt with in exactly the same way as existing staff. They will be issued with a Privacy Statement on joining as part of their induction pack.

6.2 Unsuccessful candidates and candidates who reject a job offer will have their information containing any personal details e.g. CVS, References and/or notes, securely shredded within three months of being unsuccessful, either with no interview or following an interview, and/or rejection of a job offer. This will be confirmed in a letter to the individual.

7 Managing risks

7.1 The following procedures will apply to ensure that any risks arising from obtaining, managing and processing personal information are identified early and procedures put in place to manage.

7.2 The Trustee Board will retain overall responsibly for oversight of and compliance with the data protection regulations and requirements.

7.2.1 The Trustee Board will delegate responsibility to:

- The Chief Executive (CE) as Data Controller, for the day-to- day management and control of data protection in HVA, including application of the policy and procedures, audits, risk identification and management, security, external subject access requests and any other related matters.
- HR, or the individual(s) responsible for HR, for the management and control of personal data of staff, relating to application of the policy and procedures, audits, privacy statements, risk identification and management, security, internal subject access requests and any other related matters. HR, or the HR responsible person, will report to the CE in relation to this.

7.3 HVA will undertake data information audits of all information covered by the regulations. The audits will cover: what data held, why held, whether right to consent applies, how consent will be obtained, length of period information will be held, security measures, vulnerabilities/risks and action needed to remedy gaps. See audit template at point 10.

7.4 The Chief Executive will undertake annual reviews of the data protection procedures and provide a report to the Trustee Board on the current situation with any deficiencies and action needed.

7.5 Simple Privacy or Data impact assessments (PIA) will be conducted at the beginning or in the early stages of services to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

7.5.1 The purpose of a PIA is to ensure that privacy risks are minimised while allowing the aims of the service to be met. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. Some of the ways risks can arise are through personal information being: inaccurate; insufficient or out of date; excessive or

irrelevant; kept for too long; disclosed to those who the person it is about does not want to have it; used in ways that are unacceptable to or unexpected by the person it is about; or not kept securely.

7.7 Third party suppliers who hold personal information relating to HVA on their own systems, electronic or manual, will be required to comply with HVA's data protection requirements. They will be required to sign Third-party Data Protection Agreements to confirm that any Company data is held and processed securely in line with GDPR regulation.

8 Subject access requests

8.1 Coverage and timescale

8.1.1 In accordance with legislation, staff, volunteers and service users are entitled to view their personal records, whether held in computerised or manual form. Much of the individual personal information is held electronically and staff, volunteers and service users can ask for a copy of their file to be sent to them electronically. HVA will comply with this request within 3 working days.

8.2 To gain access to any other records held by HVA, an individual must submit a written request to the CE. HVA will generally comply with requests within a month.

8.3 Rejecting a request

8.3.1 Should a staff member, volunteer, service user submit an access request(s) which HVA considers manifestly unfounded, excessive or vexatious, it has the right to charge for the administration time involved and/or reject the request, giving its reasons. Staff, volunteers or service users can appeal any decision to charge or reject. If so, they should put their appeal in writing to the CE or the Chair of the Trustee Board within five working days. Any appeal will be dealt within a timescale of ten working days, unless a different timescale is agreed with the individual.

9 Security

9.1 Information and records relating to service users will be stored securely and will only be accessible to authorised HVA personnel.

9.1.1 Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

9.1.2 It is HVA responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been destroyed or passed on/sold to a third party.

9.2 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

9.3 HVA uses various third party Data Base Systems to store data. The information held within these databases are encrypted and only accessible by HVA personnel.

9.4 There are three further areas covered:

9.4.1 Staff, Volunteers, Services Users - individuals accessing their personal information out of office should ensure where relevant that their data is viewed privately and securely, particularly in public locations.

9.4.2 Managers and administrators - similarly, managers and administrators should ensure that if they are viewing an individual's personal data outside of the office, that the data is viewed privately and securely, particularly in public locations. They should ensure that they are not physically overlooked but that their computers and any other personal devices are not accessible electronically.

9.4.3 Third party suppliers - all of these suppliers have signed Third-party Data Protection Agreements to confirm that any Company data is held and processed securely in line with GDPR and Company requirements.

10 Procedure for dealing with breaches

10.1 Breaches may arise from a number of resources e.g. complaint from an individual staff, client, supplier, the Information Commissioner's Office or a review of procedures. If a breach occurs, then it should be reported immediately to the CE. The CE will take immediate steps to close the breach. If possible, this will be done within one working day of the breach occurring

10.2 Where a breach is identified, it will be fully investigated by the CE. This may involve any or all of reviewing procedures, interviewing individuals involved or any other actions considered necessary.

10.2.1 Where possible, the investigation will be completed within ten working days. The CE will produce a written report, summarising the breach, why it occurred, how it was resolved and what further action is needed, including change of procedures, security and/or staff issues. If it is not possible to complete the report within this timetable, the CE will communicate this to the relevant parties as appropriate (e.g. Trustees, ICO, staff member) with the reasons for the delay and a revised deadline.

10.3 Following completion of any investigation, the CE will submit a Report to the Trustee Board for consideration. The Trustee Board can approve, amend, or ask for further investigation. The Trustee Board will approve the report either within ten working days of receipt or ten working days of completion of any further investigation.

10.3.1 Once approved, the CE will communicate within a further five working days writing to the other parties involved summarising the breach, why it occurred, how it was resolved and what further action is needed.

10.4 Should any disciplinary action be necessary against any individual(s) as a result of the breach, this will be dealt with in accordance with HVA's Disciplinary Procedure.

11 Data Audit

11.1 HVA will review all personal data it holds on staff, volunteers and service users on an annual basis as part of its Data Audit processes to ensure compliance as follows:

- HVA has asked individuals to positively opt in to have their personal data held by HVA.
- HVA has verified the appropriate lawful basis or legitimate interest for data processing and retention.
- HVA has specified why it wants the data and what it is going to do with that data.
- HVA informs individuals that they can withdraw their consent.

Appendices

Appendix 1 - GDPR Data Audit

Appendix 2 - Information held by HVA