Document Title:	**Data Protection Policy & Procedures**
Document Purpose:	H.A.D's. policy on Data Protection sets out the standards for H.A.D. in relation to the storage and use of personal data relating to staff, volunteers and services users.
Document Statement:	H.A.D aims at all times to comply with the Data Protection Act 2018 and the EU General Data Regulations (GDPR) on respect of data and privacy and security
Document Application:	Organisation Wide
Responsible for Implementation:	Manager and all staff
Author: **Driver:**	Rob Keene Manager
Effective date:	To be approved Drafted September 2018
Review date:	1st November 2019
Associated Documents All governing and other documentation. Human Rights Act Common Law of Confidence Act	

APPROVAL RECORD		
Agreed by Board of Trustees: **Signed: Ckelly**	Board Meeting	**Date:**

Introduction

In the United Kingdom from 25 May, 2018, security of personal data is governed by the revised EU regulations called the General Data Protection Regulations ("GDPR"), these Regulations being implemented in the UK by the Data Protection Bill. Although the GDPR is similar to the Data Protection Act 1998 ("DPA") which it replaces, there are some important differences. Unlike the DPA, the GDPR now applies to data processors as well as data controllers.

If you have any concerns as to whether there is a breach of this policy you should raise these matters in the first instance with the Manager.

All staff & volunteers are duty bound to read and understand this policy and must perform their duties and responsibilities in line with their contract of employment.

It is H.A.D's policy that all information regarding service users, clients, carers and staff members is treated as confidential and all personal sensitive information is processed under the GDPR H.A.D has a duty to notify all staff of the information contained in this policy.

Definitions

1. Personal Data	Any information relating to an identified or identifiable natural person (a Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.	
2. Special categories of Personal Data	•race; •ethnic origin; •politics; •religion; •trade union membership; •genetics;	•biometrics (where used for ID purposes); •health; •sex life; or •sexual orientation.
3. Data Controller	The entity that determines the purposes and means of processing personal data	
4. Data Processor	processes personal data on behalf of a Data Controller	
5. Privacy Notice	This sets out how we will process Personal Data, and must be given to the Data Subject at the time the data is obtained (if obtained from the data subject) or within 30 days if obtained from elsewhere.	

What does the Act cover?
The Act covers two areas:

- Giving individuals (data subjects) certain rights
- Requiring those who record and use personal information (data controllers and data processors) to be open about their use of that information and to follow sound and proper practices (the Data Protection Principles)

Lawful Basis for Data Processing
In order to process personal data there must be a valid lawful basis. Of the various legal bases available under the GDPR, there are three relevant to H.A.D as follows;

Consent - An indication of consent must be explicit (expressly confirmed in words, rather than by any other positive action) unambiguous, freely given, and involve a clear affirmative action (an opt-in). Pre-ticked opt-in boxes are specifically banned. Individual consent is required for distinct processing operations, and must specifically cover the controller's name, the purposes of the processing and the types of processing activity. This will generally be used for marketing

Contract – We may process personal data to fulfil our obligations under a contract to provide services or to fulfil a legal obligation.

Legitimate Interest - this is the most flexible of the legal bases and allows us to process Personal Data when we have a legitimate interest to do so. Because this is not tightly defined we take on extra responsibility for ensuring people's rights and interests are fully considered and protected. It requires that we use data in ways that people would reasonably expect and that have a minimal privacy impact. Examples of where we will use legitimate interest are given in our privacy notice.

We need to apply 3 tests to demonstrate our legitimate interest;
1. **Purpose test:** are we pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

1. Data Protection Policy

1.1 Scope
H.A.D's policy on Data Protection sets out the standards for H.A.D in relation to the storage and use of personal data relating to staff, volunteers and clients.

1.2 Policy Statement

1.2.1 H.A.D aims at all times to comply with its legal obligations under the Data Protection Act 2018 and the codes EU General Data Protection Regulations in respect of practice for the storage security and use privacy of personal data.

1.2.2 Personal data includes some manual records, as well as computerised records and is concerned with the processing of "personal data".

1.2.3 It is H.A.D's policy to process any personal data held in a fair and proper way, and to provide individuals with access to their own personal data if requested by the individual (Data Subject).

1.2.4 At all times H.A.D aims to ensure that personal data is kept and processed in line with the key principles under GDPR. Therefore data will be:

- Processed fairly, lawfully and transparently
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than is necessary
- Processed securely
- Not transferred to countries that does not protect personal data adequately (unless the individual has given additional consent to do this).

1.2.5 H.A.D is the data controller. (ICO Registration No. ZA230058)

Everyone who is employed by or volunteers for H.A.D. and its agencies and who processes personal data has a duty to discharge the data controller's responsibilities.

2. Personal Data Collected by H.A.D

2.1 When an employee, client or volunteer first joins H.A.D they will be asked to provide certain personal data that is required for H.A.D's records. This data will generally include the following:

- name, home address and telephone number;
- information relating to health.
- next of kin and / or emergency contact names;
- a copy of relevant certificates or licences (e.g. driving licence if driving on behalf of H.A.D.
- employment history references
- permission and contact details for contacting individuals regarding elements of H.A.D. that are of potential interest

2.2 This information is required for H.A.D's general records, to contact staff, volunteers and clients and for their health and safety.

2.3 H.A.D may also request further details about an individual's general health in order to ascertain their ability to undertake their role or to take part in activities

3. Special Categories of Personal Data (Sensitive Data)

3.1 H.A.D does keep certain sensitive data on staff, volunteers and clients. Sensitive data held and the reasons for this have been summarised below:

Examples of sensitive data and reasons held

Personal Data	**Reason for Holding Data**
Health / sickness records	To ensure the persons health and safety in carrying out the job role
Disabilities	To facilitate adaptations / reasonable adjustments in the work place
Ethnic origin	To ensure equality of opportunity Commission or alleged commission of To comply with government standards

3.2 All data is treated in the strictest confidence and access to sensitive data will be restricted and kept securely at all times.

3.3 H.A.D does not need consent to process special categories of their personal data when processing it for the following purposes:

- Where it is necessary to protect the individual's vital interests or those of another person
- where you/they are physically or legally incapable of giving consent
- Where staff or volunteers have made the data public
- Where processing is necessary for the establishment, exercise or defence of legal claims
- Where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity

4. Data Security

4.1 All staff and volunteers are expected to take all reasonable precautions and follow H.A.D's policy and best practice to ensure the security and integrity of personal data held and processed by H.A.D

4.2 Personal data is kept securely at all times.

4.3 Manual files are kept in a locked filing cabinet and may be accessed only by authorised personnel.

4.4 Employees must not leave paper with personal data lying about, nor should they take personal data away from H.A.D's premises without the explicit permission of their manager. Personal data should be shredded and disposed of securely when it has been finished with.

4.5 Data kept on computer systems is password controlled/protected.

4.6 Personal data must not be saved to any personal computers or devices.

5. Manging Data Breaches

5.1 In the event of a breach, it is vital that appropriate action is taken to minimise associated risks. Any breach must be notified immediately to the Manager and the Chair of the Board of Trustees and the board trustee responsible for GDPR procedure. ***There are strict timescales for making notifications to the ICO and/or the Data Subject, and depending on the nature of the breach must be notified within 72 hours of the breach being identified***

Examples of breach incidents include but are not limited to:-

- Loss of any data which is identifiable to any client, member of staff or volunteer be it a paper file or held on an electronic device (e.g. laptop/USB memory stick)
- Awareness of any confidential data that has not been lost, but has been disposed of incorrectly (not shredded) that relates to any client, member of staff, or volunteer.
- Disclosure of Personal Data to a party not entitled to receive it
- IT incidents involving personal data e.g. processing failures, hardware failures, website failures, IT outages etc.
- Information security incidents e.g. file losses (accidental or theft), email breaches, loss of laptops, unauthorised disclosure of or access to data, loss of data through deception, hacking/virus attack, phishing etc.
- Building issues – e.g. a break in or vandalism leading to a security risk, staff threats.

5.2 An investigation into the breach will commence within 24 hours of the breach being discovered and an appropriate course of action will be determined and recommended to the board of trustees.

5.3 Data breach notifications to the ICO shall include the following information:-

- The categories and approximate number of Data Subjects concerned;
- The categories and approximate number of Personal Data records concerned;
- The name and contact details of H.A.Ds data protection officer.
- a description of the likely consequences of the Personal Data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the Personal Data breach, and mitigate any possible adverse effects

5.4 Breach notifications to affected data subjects need to describe, in clear and plain language, the nature of the personal data breach and, at least:-

- the name and contact details of our data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the Personal Data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the Personal Data breach and mitigate any possible adverse effects.

6. Auditing

6.1 H.A.D will audit personal data on a regular basis and ask staff, volunteers and clients to confirm the accuracy of data held. Staff, volunteers and clients are asked to co-operate with any auditing process implemented to ensure the accuracy and completeness of data held.

6.2 Auditing may take the form of providing staff, volunteers and clients with a copy of certain personal data held and asking volunteers to confirm the accuracy of this data.

7. Data Sharing and Subject Access Requests

7.1 This section sets out the procedure for handling data sharing requests and subject access requests, in order to comply with an individual's rights under the GDPR to access to their data.

Requests to access or share personal data are most likely to be received from the Data Subject themselves (known as Data Subject Access requests) or the Police. Requests may also come in from other third parties as well. All requests must be referred to the Manager.

7.2 - Handling Data Subject Access Requests
Information must be provided:-

- free of charge, unless manifestly unfounded or excessive - a reasonable fee (which can only be the actual administration costs incurred) can be charged if such requests are repetitive.
- without delay; and at the latest within one month of receipt (which can be extended by two months where complex).

7.3 Information will only be provided to other third parties where the data subject has consented or there is a legal obligation to do so, or where this is part of a possible legal transaction involving H.A.D.

7.4 All staff, volunteers and clients may apply for a copy of the personal data held on them by H.A.D. If any information is incorrect, H.A.D is committed to correcting this without undue delay. H.A.D requests that all staff and volunteers inform them of any changes in personal data or circumstances that may be relevant to their time with H.A.D.

7.5 If anyone wishes to see a copy of information held on them, H.A.D.'s preferred method of request is in writing to the Manager, however we will also except a verbal or electronic request to a member of staff.

7.6

- A data subject has the right to request that we erase their personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. Any such request should be made to the Manager.

- Whilst requesting that their personal data is corrected or erased or are contesting the lawfulness of our processing, a data subject can apply for its use to be restricted while the application is made. Any such request should be made to the Manager

- A data subject has the right to object to data processing where we are relying on a legitimate interest to do so and they think that their rights and interests outweigh our own and they wish us to stop.

- A data subject has the right to object if we process their personal data for the purposes of direct marketing.

- A data subject has the right to receive a copy of their personal data and to transfer their personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

- With some exceptions, a data subject has the right not to be subjected to automated decision-making

- A data subject has the right to be notified of a data security breach concerning their personal data.

7.7 Handling Data Requests from the Police

Any request for personal data by the police must be referred to the manager and must also be agreed by the Chair of the board of trustees.

8. CCTV

8.1 Common CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act 2018.

8.2 H.A.D's system comprises a number of fixed cameras located both internally and externally around the premises. All cameras may be monitored and are only available for use by approved members of staff.

8.3 The objectives of the CCTV system are:-

- To protect the building and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption
- To increase the personal safety of staff and visitors and reduce the fear of physical abuse, intimidation and crime.
- To assist in identifying, apprehending and prosecuting offenders on the premises
- To protect members of the public and private property.

8.4 HAD will comply with the Data Protection Act 2018, whether it be information, recordings and downloads which relate to the CCTV system.

8.5 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the HAD CCTV.

8.6 Access to the CCTV will be strictly limited to the members of staff approved by the Executive Principal.

8.7 Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals.

8.8 Video Download Procedures.

- Recordings may be viewed by the police and authorised officers for the prevention and detection of crime. Permission to do this will be given from the Chair of the Board of Trustees.

- A record will be maintained of the release of downloads to the police or other authorised applicants. A register will be available for this purpose and will be kept by the Manager.

- Viewing of downloads by the police must be recorded in writing and in the register. Requests by the police can only be actioned under section 29 of the Data Protection Act 2018.

- Should a download be required as evidence, a copy may be released to the police under the procedures described in the above paragraphs of this Policy. Downloads will only be released to the police on the clear understanding that the disc remains the property of the HAD, and both the disc and information contained on it are to be treated in accordance with this Policy. HAD also retains the right to refuse permission for the police to pass to any other person the disc or any part of the information contained thereon.

- Applications received from outside bodies (e.g. solicitors) to view or release downloads will be referred to the Chair of the Board of Trustees. In these circumstances downloads will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject

access request, or in response to a Court Order. A fee of £100. can be charged in such circumstances.

- Images are stored for 30 days and then deleted.

9. Marketing

9.1 Marketing activity is primarily governed by the Privacy and Electronic Communication Regulation (PECR) which needs to be observed in conjunction with the GDPR recognising the rights of individuals and the legal bases for processing. There are specific rules on:-

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

PECR restrict unsolicited marketing by phone, fax, email, text, or other electronic message with different rules for different types of communication. The rules are generally stricter for marketing to individuals.

9.2 H.A.D's marketing activities will be limited to:-

- Informing existing clients about services and activities we believe may be of interest to them
- Informing former clients who previously used our services but no longer do
- Informing prospective clients that have approached us about our services or activities.

9.3 We will provide the Data Subject with a copy of our privacy notice within 30 days of receiving/holding data or when we first make contact (whichever is sooner) and offer opt out / respect requests not to be contacted further.

9.4 Our legal basis for processing will always be on using Legitimate Interest

10. Complaints or Concerns about Data Protection

10.1 If a member of staff, volunteer or client has concerns about any matters relating to data protection (e.g. the way data is stored, data held, or use of data), they should initially raise this with the Manager.

10.2 All complaints received will be referred to the chair of the board of trustees