



Herts Disability Sports Foundation

Registered Charity No. 1156034

Data Management Policy

Version control : 1.0

Date of Policy – July 2018

Date for Review – July 2021

Approved Date

(Signature of Chair)

Herts Disability Sports Foundation – Data Management Policy

Contents	2
Introduction.....	3
Data Protection Principles.....	3
Types of Data we hold	4
Responsibilities (and contact details).....	4
Access to Data	5
Data Security	5
Third Party Processing.....	5
Requirement to Notify Breaches.....	6
Training.....	6
Information Asset Register at July 2018.....	7
- Annex A - Employees	7
- Annex B - Trustees	8
- Annex C - Members of the Public	9

Introduction

1. HDSF collects a range of personal information about people we work with; employees, Trustees and members of the Public. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

Personal data is any information about a person who can be identified, directly or indirectly, through the information – by use of a name or a code linked to that individual (such as a NI number).

2. We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly. We welcome feedback about any of our procedures for handling personal data – it will help us improve and ensure we maintain the highest standards.

3. We have created Privacy Notices for Trustees, Employees and Members of the Public which provide the detail on what information we collect, why we collect it, what we do with it, rights relating to that information and how we ensure the security of information we store. This is also listed in our Information Asset Register. If there are changes to the information we collect or what we use it for, the Privacy Notices and Information Asset Register will be updated.

4. This policy confirms the principles and procedures we will apply to ensure that all data is collected legally and is managed in accordance with best practice as provided in the General Data Protection Regulation (GDPR) and advice from the Information Commissioner's Office. We have registered with the ICO and will renew our registration annually.

5. Where any of the HDSF policies refer to data protection, this should be read to include the provisions of GDPR.

Data Protection Principles

6. Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- a) processing will be fair, lawful and transparent,
- b) data be collected for specific, explicit, and legitimate purposes,

- c) data collected will be adequate, relevant and limited to what is necessary – we will only collect data if we actually have a need to,
- d) data will be kept accurate and up to date. Data which is found to be inaccurate will be corrected or erased as quickly as possible,
- e) data is not kept for longer than is necessary for its given purpose,
- f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures,
- g) we will comply with the relevant GDPR procedures for international transferring of personal data.

Types of Data we hold

7. A copy of our most recent Information Asset Register is attached to this policy at Annex A. This will be updated if there are any changes.

8. We will review our Register annually or when there are any changes – to check that procedures are being followed and that information is being used and stored as described.

Responsibilities

9. We have appointed a Data Controller;

Sine Bates
Herts Disability Sports Foundation
c/o Knights Templar School
Park Street
Baldock
Herts SG7 6DZ
Telephone number – 01462 600193
Email – bates.hdsf@yahoo.com

She is your first point of contact for any questions or enquiries about your data.

10. If you are not happy with the response you are given, you should contact our Senior Information Risk Officer, Maria Anastase, who is one of our Charity Trustees. She can be contacted through the Chair of Trustees at;
nigel.kippax@charityleaders.org.uk

Access to Data

11. Employees, Trustees and Members of the Public have a right to access the personal data that we hold on them. To exercise this right, they should contact our Data Controller - we will comply with the request as quickly as possible, ideally within one week. If it will take longer, we will communicate the reason for the delay and provide an estimate of how long it will take.

12. No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge may be applied.

Data Security

13. All our employees are aware that hard copy personal information should be kept in a locked room, filing cabinet, drawer, storage wallet or safe. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

14. Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

15. Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

16. Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Third Party Processing

17. Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

Requirement to Notify Breaches

18. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

19. The following are examples of data breaches:

- a) access by an unauthorised third party;
- b) deliberate or accidental action (or inaction) by a data controller or data processor;
- c) sending personal data to an incorrect recipient;
- d) computing devices containing personal data being lost or stolen;
- e) alteration of personal data without permission;
- f) loss of availability of personal data.

20. In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by (either by the Data Controller or the Senior Information Risk Officer) who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

21. All data breaches will be recorded on our Data Breach Register. Where legally required (a breach which is likely to pose a risk to people's rights and freedoms), we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

22. HDSF records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken. Details of all breaches will be provided to the Board of Trustees.

Training

23. New employees must read and understand this policy as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

Information Asset Register – July 2018 – Employees

Annex A

Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	Link to contract with processor	Retention schedule (if possible)	General description of technical and organisational security measures (if possible)	Article 6 lawful basis for processing personal data	Rights available to individuals	Location of personal data
Finance	Payroll	N/A	Employees	Contact details	HDSF Admin Manager, HMRC, Numerus and NEST	Numerus contract and consent form	5 years post-employment	Encrypted storage	Article 6(1)(b) - contract	Access, data portability, rectification	HR personnel file (paper) and encrypted HR memory stick
Finance	Payroll	N/A	Employees & Volunteers	Bank details	HDSF Admin Manager, 2nd bank signatory	N/A	3 years post-employment	Encrypted storage and transfer	Article 6(1)(b) - contract	Access and rectification	HDSF Bank account
Finance	Audit	N/A	Employees	Bank details	External examiner, Fin staff KTS	N/A	5 years post-employment	file in locked room	Article 6(1)(c) - legal obligation	Access	Bank statements, finance folder
Finance	Payroll	N/A	Employees	Pension details	HDSF Admin Manager, HMRC and NEST	NEST tbc	75 years post-employment	Encrypted storage and transfer, file in locked room	Article 6(1)(c) - legal obligation	Access, data portability, rectification	NEST website, Finance folder - paper copy
Finance	Payroll	N/A	Employees	Tax details	HDSF Admin Manager, HMRC, Numerus	Numerus contract	6 years post-employment	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	Access, data portability, rectification	Payroll Spreadsheet
HR	Payroll	N/A	Employees	Pay details	HDSF Admin Manager, 2nd bank signatory, HMRC, Numerus and NEST	Numerus contract, NEST tbc	6 years post-employment	Encrypted storage and transfer, file in locked room	Article 6(1)(b) - contract	Access, data portability, rectification	Payroll Spreadsheet and Payroll folder
Resource Management	Training	N/A	Employees & Volunteers	Record of trg and dates	HDSF employees	N/A	5 years post-employment	Encrypted storage	Article 6(1)(b) - contract	Access, data portability, rectification	Training spreadsheet
Resource Management	Weekly rota	N/A	Employees & Volunteers	Rota for all 'delivery' staff and volunteers	All HDSF employees and volunteers	N/A	6 years post-employment	File locked in room	Article 6(1)(b) - contract	Access, data portability, rectification	Payroll folder
HR	Risk Management	N/A	Employees	Next of Kin details, medical conditions and allergies and GP details.	HDSF Admin Manager	N/A	5 years post-employment	Encrypted storage	Article 6(1)(d) - vital interest	Access, data portability, rectification	HR personnel file (paper) and encrypted HR memory stick

Information Asset Register – July 2018 – Trustees

Annex B

Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	Retention schedule (if possible)	General description of technical and organisational security measures (if possible)	Article 6 lawful basis for processing personal data	Rights available to individuals	Location of personal data
Human Resources	Recruitment	N/A	Trustee	Contact details	Charity Secretary	10 years post resignation	Kept in cupboard in locked room	Article 6(1)(b) - contract	Access	Paper copy in Trustee folder
Human Resources	Recruitment	N/A	Trustee	Qualifications	Charity Secretary	10 years post resignation	Kept in cupboard in locked room	Article 6(1)(b) - contract	Access	Paper copy in Trustee folder
Human Resources	Recruitment	N/A	Trustee	Employment history	Charity Secretary	10 years post resignation	Kept in cupboard in locked room	Article 6(1)(b) - contract	Access	Paper copy in Trustee folder
Human Resources	Recruitment	N/A	Trustee	References	Charity Secretary	10 years post resignation	Kept in cupboard in locked room	Article 6(1)(b) - contract	Access	Paper copy in Trustee folder
Compliance	Financial audit	N/A	Trustee	Declaration of pecuniary interests	Charity Secretary & Chair of Trustees	10 years post resignation	Kept in cupboard in locked room	Article 6(1)(c) - legal	Access, rectification	Paper copy in Trustee folder

Information Asset Register – July 2018 – Members of the Public

Annex C

Business function	Purpose of processing	Name and contact details of joint controller (if applicable)	Categories of individuals	Categories of personal data	Categories of recipients	Link to contract with processor	Retention schedule (if possible)	General description of technical and organisational security measures (if possible)	Article 6 lawful basis for processing personal data	Rights available to individuals	Location of personal data
Sales (Holiday activities consent form)	Health & Safety	N/A	New and Existing customers	Contact details of parent/guardian, medical details and age.	HDSF employees	N/A	3 years, reviewed annually	Kept in padlocked folder	Article 6(1)(a) - consent	Access, data portability, rectification, objection, erasure	Paper copy of consent form is kept in a padlocked folder, anonymised data on password protected spreadsheet
Sales (Holiday activities consent form)	Marketing	N/A	Existing customers	Permission to use personal images.	HDSF employees	N/A	3 years, reviewed annually	Kept in padlocked folder	Article 6(1)(a) - consent	Access, data portability, rectification, objection, erasure	Paper copy of consent form is kept in a padlocked folder
Sales (Holiday activities website booking)	Contract	N/A	New and Existing customers	Parent/guardian; name, phone number. Child; name, age, disability and any medical conditions.	HDSF employees	https://www.wix.com/about/privacy	On website it is deleted at end of week of sessions, anonymised data transferred to spreadsheet	Website password protected.	Article 6(1)(b) - contract	Access, data portability, rectification, objection, erasure	Wix website is password protected. Spreadsheet is password protected.
Sales - Newsletter	Marketing	N/A	New and existing customers	email address	HDSF employees	https://mailchimp.com/legal/privacy/	Until asked to remove	Website password protected.	Article 6(1)(a) - consent	Access, data portability, rectification, objection, erasure	Paper copy of consent on file in locked room, email address password protected on mailchimp website
Sales (Open sessions)	Contract	N/A	New and existing customers	Name, age and whether they have a disability	HDSF employees	N/A	Register destroyed once info transferred to password protected spreadsheet.	Info on register anonymised and transferred to spreadsheet.	Article 6(1)(b) - contract	Access, rectification, objection, erasure	Anonymised data on password protected spreadsheet.
Reporting on Grant Funding	Audit	N/A	Customers receiving a service that is grant funded	Name, gender, age, ethnicity, location of sessions and attendance at sessions	HDSF employees	Information is anonymised before it is provided to external grant funding bodies	Period of grant funding plus 1 year.	Spreadsheet password protected.	Article 6(1)(b) - contract	Anonymised	Spreadsheet
Sales (Daycare services)	Contract	N/A	New and existing customers	Name, gender, age, ethnicity, location of sessions and attendance at sessions - info provided by DS staff	HDSF employees	N/A	Register destroyed once info transferred to password protected spreadsheet and any relevant invoice issued.	Electronic register password protected.	Article 6(1)(b) - contract	Access, data portability, rectification, objection, erasure	Spreadsheet