Data Protection Policy

Introduction

Hyde Park Source (HPS) is a data processor, we collect, store and use information about Data Subjects (employees, volunteers and service users) who we come into contact with in order to carry out our work. This information must be handled (collected, stored, used and disposed of) in line with:

- The Data Protection Act 1998,
- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation (GDPR) 2018.

All staff must be informed of our data protection policy and asked to sign a compliance form on induction (see appendix 1).

Our named Data Protection Officer is **Pete Tatham** **pete@hydeparksource.org**

In line with the Data Protection Act 1998 principles, HPS will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

Data Processor

HPS must apply one of the following legal grounds to be able to process (use) your personal information:

- **Consent** (e.g. on a registration form)
    - Must be freely given
    - This consent will usually last for 1 year unless it is directly linked to a project/funder which is over this time period
    - Can be withdrawn by phoning 0113 245 8863 or emailing our data protection officer.
- **Legitimate Interest**
    - If we have a genuine legitimate reason to do so

        - To inform you of a new opportunity or event which furthers the aims and objectives of HPS.
            - You will always be given the opportunity to update preference for this contact.
    - It does not harm any of your rights and interests as an individual

Legal Obligation

- If we are required to by law, for example due to a Safeguarding concern or allegation.

- **Vital Interest**
    - In extreme situations such as an emergency we would share relevant details with the emergency services for the preservation of life.

Data Storage and Protection

We store data at HPS securely:

- In a locked filing cabinet in our office
- In a password protected database(s)
- Photos are stored in password protected folders
- If project workers have personal information on work mobiles these are password protected
- Where the transit of data is necessary, all USB sticks are encrypted
- If we are not at our computer, we will lock it or log out
- All computers automatically log off after 30 minutes
- All cloud based data is stored on servers which comply with UK GDPR laws
- If staff have collected data on site or need to bring data out on site (registers Emergency contact info), information will be kept within the staff members bag in an envelope/opaque folder and the member of staff must have their bag locked in a room or on their person whilst these details are not stored at our office.

Data Access and Accuracy

All Data Subjects have the right to access the information HPS holds about them. HPS will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Types of Data

HPS processes the following types of data, which is stored both on paper and on a server:

Personal and sensitive information

<u>Volunteers:</u>

- Your name, date of birth, address, contact details
- An emergency contact
- Relevant information about your health & welfare
- Pictorial data
- We may also need information about previous convictions if relevant and not 'spent', if so, we may also need to keep records of regular reviews
- For anyone working with children we will need DBS information
- Equal opportunities monitoring data
- Equal opportunities monitoring data is kept separate to personal data

Staff, including sessional staff:

- National Insurance number
- Bank details
- Contact details
- Emergency contact
- Supervision and appraisal notes
- Sick notes
- Record of sickness, absence and holiday leave

HPS Job applicants

- Information contained in prospective employee application forms
    - Job applications are kept for 1 year in line with the Civil Rights Act of 1964.

What we use it for:

- To contact you, or someone else in case of an Emergency
- To keep everyone safe whilst volunteering and working with us and to pass on to Emergency services in case of an accident or ill-health
- To promote the work we do e.g. via social media, our website, newspapers and newsletters
- To monitor projects and feedback to our funders

What we do with it:

All data is processed and stored securely (see details above) within the UK. No 3rd parties have access unless the law allows them to, i.e. in the case of a Safeguarding and/or Police investigation) or unless we make this clear on the registration form (for partnership work).

How long we keep it:

Volunteers

We only keep your data for as long as necessary either:

- The length of time you are an 'active' volunteer with HPS
    - If you have not attended a weekly group for 4 weeks we will try to contact you via phone/text/email to ask if you wish to receive the weekly group-reminder texts.
    - For more irregular volunteers (e.g. monthly) we will contact you annually (each December) to ask if you would like remain on our system.
- For the duration of the funded project you have registered as part of, and if your data is necessary for our monitoring purposes.
- We will keep your e-mail contact details on our mailing lists (if you subscribe on the application form) until you notify us that you no longer want to receive the information.

Staff

We will only keep your details for as long as necessary. Details required for payroll will be destroyed after your last payment. Other information such as sickness records, may be kept for up to 6 years after you have left HPS for legal reasons.

Your Rights: You can request to see the information we hold or ask to have it corrected/deleted at any time. If you wish to raise a complaint, contact our Data Protection Officer, if you are not satisfied/believe we are processing un-lawfully you can complain to the Information Comissioner's Officer (ICO).

Due to the nature of our data processing we are exempt from registering with the ICO, this is because we:

- only process information necessary to establish/maintain membership/support;
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- only share the information with people and organisations necessary to carry out the organisation's activities.
- only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration.

We are responsible for notifying the Information Commissioner with regards to any potential or actual breach of this policy.

Access to IT devices

HPS staff use computers in the office to access data.

To ensure data is secure all computers:

- Automatically log off after 15 minutes of inactivity
- Are password protected
- Passwords are changed when any member of staff leaves the organisation
- Have a guest log in, for use by HPS volunteers

Staff may keep personal information on their work mobile phones. To keep data secure all staff must:

- Have access to a work-only phone or SIM card
- Password protect their phone
- Move work-related photos stored on the phone onto the work server on a monthly basis and delete photos from their phone.

Disclosure

HPS will never sell or swap your data. We are unlikely to share data with other organisations, but in circumstances where this is required (e.g. due to partnership work), the Data Subject will be asked for consent and made aware of how, what and with whom their information will be shared.

There are circumstances where the law allows HPS to disclose data without the data subject's consent- these are:

- Carrying out a legal duty as authorised by an appropriate legal officer.
- The Data Subject has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.

HPS places great importance on the correct treatment of personal information as a key element in the success of our working relationships, and in maintaining the confidence of those with whom we deal. Hyde Park Source intends to ensure that personal information is treated lawfully and correctly.

In addition, HPS will ensure that:

- It has a Data Protection Officer: **Pete Tatham** with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- It deals promptly and courteously with any enquiries about handling personal information (legal limit 40 days).
- It describes clearly how it handles personal information.
- It will review and audit the ways it holds, manages and uses personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

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 1998 and General Data Protection Regulation 2018.

In case of any queries or questions in relation to this policy please contact the HPS Data Protection Officer **Pete Tatham.**

The following list below of definitions of the technical terms it has used is intended to aid understanding of this policy.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998, GDPR 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g. name, address, photograph, contact details, IP address

Sensitive data – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings relating to a data subject's offences

Data Protection Policy
Appendix 1

Staff member:

By signing this form, I agree to the following:

1.	I will use a password protected log in to access work-related data from work computers
2.	I will use a password protected log in to access work-related data from a personal device
3.	If accessing the work server from a personal device I will log out immediately after use
4.	I will not share my log in details with anyone
5.	I will not store work related images on my phone (work or personal) for more than a month

Signed: Date:

Data Protection Policy
Appendix 2

HPS processes personal and sensitive data. Every care is taken to protect the data we hold from both an accidental and/or deliberate data protection breach.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

In the event of a data breach regarding any personal data processed by HPS, we will carry out our Data Breach Procedure.