HALTWHISTLE PARTNERSHIP LTD

DATA PROTECTION AND THE MANAGEMENT OF SENSITIVE INFORMATION

SCOPE OF POLICY

This policy applies to all staff, trustees, volunteers, service users and contractors. Each project team or individual that handles personal data must ensure it is handled and processed in line with this policy and data protection principles.

AIM OF THE POLICY

To comply with the law, ensuring that personal information is collected and used fairly, stored safely and not disclosed unlawfully.

Introduction

Haltwhistle Partnership (hereafter HP) needs to gather and use certain information about individuals. These can include volunteers, members, service users, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet data protection standards – and to comply with the law.

This data protection policy ensures HP:

- Complies with data protection law and follows good practice
- Protects the rights of staff, trustees, members, volunteers, service users and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

The policy applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include sensitive information such as:

- Names, addresses, contact details including next of kin
- CVs and other information gathered during recruitment
- Medical or health information
- Financial records including National Insurance number, tax codes
- Sexual orientation
- Religion

What is the general data protection regulation (GDPR)?
Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

People with key areas of responsibility:

The Trustees ultimately responsible for ensuring that HP meets its legal obligations.

The designated Data Compliance Officer is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection training and advice for the people covered by this policy
- Handling data protection questions from staff, volunteers and anyone else covered by this policy.
- Dealing with requests from individuals to see the data HP holds about them (also called 'Subject Access Requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services HP is considering using to store or process data, for instance cloud computing services.

- Approving any data protection statements attached to communications such as email and letters.

General guidelines for trustees, employees, contracted workers and volunteers

- New trustees, employees, contracted workers and volunteers must read the policies on data protection as part of their induction.
- All trustees, employees, contracted workers and volunteers receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.
- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Trustees, employees, contracted workers and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and never shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date or no longer required, it should be deleted and disposed of safely.
- Trustees, employees, contracted workers and volunteers should request help from their line manager or the HP Data Compliance Officer if they are unsure about any aspect of data protection.

How and where data should be safely stored

When data is stored on **paper**, it should be kept in a secure place where unauthorised people cannot see it. This also applies to data that is usually stored electronically but has been printed out for a reason. The following must be followed:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Trustees, employees, contracted workers and volunteers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored **electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between trustees, employees/contracted workers/ volunteers.
- If data is stored on removable media (like a CD or USB stick) these should be kept securely when not being used.
- Data should be backed up regularly in line with the HP standard backup procedures.
- Laptops, digital tablets, phones or USB drives should never be left unattended where they are at risk of being stolen.
- All servers and computers containing data should be protected by approved security software.

Data use

When personal data is accessed and used it can be at greatest risk of loss, corruption or theft:

- When working with personal data, employees and volunteers should ensure the screens of their computers or device are always locked when unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email unless encrypted as this form of communication is not secure.
- Trustees and employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Trustees, employees and volunteers who hold personal data (electronically or on paper) to be able to carry out their role must ensure it is securely held at all times.

Data accuracy

The law requires HP to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all trustees, employees and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Trustees, staff and volunteers should not create any unnecessary additional data sets.
- Trustees, staff and volunteers should take every opportunity to ensure data is kept up to date.
- HP will make it easy for data subjects to update the information HP holds about them. For example via Mailchimp contact details or by phoning the office on 10434 321242.
- Data should be updated as inaccuracies are discovered. For instance, if a data subject can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by HP are entitled to:

- Ask what information HP holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts HP requesting this information, this is called a 'Subject access request'. Subject access requests from individuals should be made in writing by email, addressed to admin@haltwhistle.org or by post to the Administrator, Haltwhistle Partnership, Westbourne House, Main Street, Haltwhistle, Northumberland NE49 0AZ.

Individuals will not be charged for a subject access request. The Data Compliance Officer will provide the relevant data within 1 month. However, a 'reasonable fee' can be charged if the request is manifestly unfounded, excessive, or repetitive. A reasonable fee can also be charged to comply with requests for further copies of the same information. This does not mean that HP can charge for all subsequent access requests. Any reasonable fee must be based on the administrative cost of providing information.

The Data Compliance Officer will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

HP may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows HP to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State.
2. Protecting vital interests of a Data Subject or other person.
3. The Data Subject has already made the information public.
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion.
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Under these circumstances HP will disclose requested data. However, the Data Compliance Officer will ensure the request is legitimate, seeking assistance from the trustees and from HP's legal advisers where necessary.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of HP becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, HP will do so without undue delay.

Providing information

HP aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, HP has a privacy policy, setting this out.

Data Protection Compliance

The designated Data Compliance Officer is the organisation's appointed compliance officer in respect of its data protection activities. He / she can be contacted via admin@haltwhistle.org

Issued: July 2022
Reviewed: April 2023
Revised: November 2023