Data Protection and the Management of Sensitive Information Policy

Haltwhistle Partnership Limited

A charitable company limited by guarantee

Westbourne House, Main Street
Haltwhistle, NE49 0AZ
Ph: 01434 321242

www.haltwhistle.org

admin@haltwhistle.org

SCOPE OF POLICY

This policy applies to all staff, trustees, volunteers, service users, contractors, and others handling personal data on behalf of the Haltwhistle Partnership. 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

This policy outlines how the Haltwhistle Partnership complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) in its handling of personal and sensitive information. It ensures that data is collected, processed, stored, and disposed of lawfully and ethically.

PURPOSE OF THE POLICY

The purpose of this policy is to ensure that trustees, staff and volunteers are aware of their individual responsibilities in relation to data protection, processing data, confidentiality, and the management of sensitive information within the Haltwhistle Partnership. The policy identifies the rules governing access to personal information and sensitive information management. The importance of data protection and confidentiality will be reinforced during trustee, staff and volunteer induction procedures.

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

LEGAL FRAMEWORK

This policy complies with:

- UK GDPR
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Relevant guidance issued by the Information Commissioner's Office (ICO)

DEFINITIONS

Term	Definition
Personal Data	Any information relating to an identified or identifiable person.
Special Category Data	Sensitive data including racial or ethnic origin, political opinions, religious beliefs, health data, sexual orientation, etc.
Processing	Any operation performed on personal data (e.g. collection, storage, use, deletion).
Data Compliance Officer	The Administrator is appointed by the trustees as an advocate for the proper care and use of information
Data Subject	The individual whose data is being processed.
Data Controller	The Haltwhistle Partnership is responsible for how and why personal data is processed.
Data Processor	A third party processing data on behalf of the controller.
Data Protection Impact Assessment (DPIA)	An assessment of the impact of any planned processing operations on the protection of personal data.
Disclosure	The passing of personal data to a third party, either by an individual or the organisation.
Subject Access Request	The right of a data subject to have access to the information held about them.

DATA PROTECTION PRINCIPLES

Under the Data Protection Act, 2018, and Article 5 of UK GDPR, personal data must 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.

LAWFUL BASES FOR PROCESSING DATA

We process data only where a lawful basis applies:

- Consent (freely given and documented)
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests (after assessment)

Where processing **Special Category Data**, we must meet one of the conditions in **Article 9 of UK GDPR**, such as:

- Explicit consent
- Employment or social protection law
- Substantial public interest
- Legal claims
- Safeguarding

Safeguarding Policies are maintained for data processing relevant to HP activities, as required by the DPA 2018.

ROLES AND RESPONSIBILITIES

- **Trustees** ensure governance-level oversight.
- **The Data Compliance Officer** oversees compliance, compliance, and breach handling.
- **All staff and volunteers** must understand and comply with this policy, and sign a Data Protection Agreement during induction.

The Trustees are ultimately responsible for ensuring that HP meets its legal obligations. The HP Administrator is the designated Data Compliance Officer, and is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection induction 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, STAFF, 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.

DATA COLLECTION, STORAGE, MANAGEMENT AND USE

We collect and use personal data for:

- Delivering services to beneficiaries
- Managing staff, volunteers, and trustees
- Fundraising and donor management
- Monitoring and evaluation
- Regulatory compliance (e.g. HMRC for Gift Aid)

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.

Sensitive data is only collected when strictly necessary and with a clear lawful basis. It is stored securely, and access is restricted to those with specific roles. Where data relates to health, ethnicity, or safeguarding, additional safeguards are applied. A Data Protection Impact Assessment (DPIA) will be conducted for high-risk processing activities.

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.

We apply appropriate technical and organisational measures including:

- Password protection and encryption
- Secure file storage (e.g., cloud platforms with two-factor authentication)
- Access controls
- Staff and volunteer training
- Secure disposal of data

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.

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 WhatsApp contact details or by phoning the office on 01434 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

Individuals have the following rights under UK GDPR:

- Access to their data
- Rectification of inaccurate data
- Erasure of data ("right to be forgotten")
- Restriction of processing
- Data portability
- Object to processing
- Not to be subject to automated decision-making
- Withdraw consent (where applicable)

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.

RETENTION AND DISPOSAL

Personal data will be retained only as long as necessary and in accordance with our **Data Retention Schedule**. Data is securely deleted or destroyed when no longer required.

DISCLOSURE

- Personal data will only be shared where legally permitted and necessary (e.g., with funders, regulators, IT providers).
- Contracts with data processors include GDPR-compliant terms.
- No data will be sold or shared for marketing without consent.

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

All data breaches must be reported to the Data Compliance Officer. 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 (ICO) 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.

DATA PROTECTION INDUCTION

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.

All staff and volunteers are required to acknowledge that they have read, understood, and agreed to comply with this policy by signing the Data Protection Agreement.

DATA PROTECTION COMPLIANCE

The Haltwhistle Partnership's appointed Administrator and Compliance Officer, Samantha Dalglish, serves as the designated Data Compliance Officer responsible for data protection activities. She can be contacted via admin@haltwhistle.org

Issued: July 2025

We are committed to regularly reviewing our policy.

This policy will be reviewed every three years or sooner if there is a change in legislation or there is applicable learning from a critical incident.

Any changes made to new policies will be circulated to all concerned.

Next review date: July 2028

Dated Reviewed	Reviewed by