



## Data Protection Policy

Contents	
Introduction and Scope.....	1
Need for Data Protection Policy.....	2
The Principles of Data Protection .....	2
Complying with the Principles of Data Protection .....	3
The Rights of Data Subjects .....	3
Our Guarantees:.....	3
Disclosure and Barring Service .....	4
Storage and Access.....	4
Handling .....	4
Usage .....	4
Retention .....	4
Disposal.....	4
Applying the Data Protection Policy.....	4
Protecting Data from unauthorised use, loss or unlawful disclosure.....	5
Review and Audit of Policy .....	5
Training.....	5
Registration with Information Commissioners Office (ICO).....	5
Data Protection Officer .....	5

### Introduction and Scope

Heart of Hastings (HOH) has robust policies and procedures in place to ensure that we comply with the General Data Protection Regulations 2016 (GDPR) in all our dealings with data subjects.

- We will regularly update and make publically available our data protection policy.
- We process data only as necessary for the completion of our activities, and limit access to personal data within the organisation to those officers who require it.
- HOH follows Privacy by Design principles ensuring that it's office and ICT systems protect data subjects interests in accordance with GDPR.
- HOH recognises that Data Protection is a dynamic process and so references data protection in a number of documents across it's activities.

The full list is referenced in the Data Audit and Documentation document and includes:

- Privacy Notice (internal data subjects)
- Data Processors Agreement (and email guidance)

HEART OF HASTINGS CLT Limited

Registered with the FCA: N° 7604 Registered Charity with HMRC N° EW82493.

Registered address: Rock House, 49-51 Cambridge Road, Hastings

TN34 1DT

GDPR Policy  
Filming and Photography Disclaimer  
Data Subject Notice (Stalls)  
Web Data Use Statement  
Staff Handbook  
Contact of Employment

## **Need for Data Protection Policy**

In order to operate efficiently, HOH has to collect and use information (data) about people with whom it works. These may include current, past and prospective employees; past and prospective volunteers; supporters and third party organisations such as staff payroll services or organisations we have an alliance with. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal data HOH gathers is handled and dealt with in accordance with GDPR, including data collected on paper, face to face, or via internet including through social media.

HOH fully endorses and adheres to the principles of data protection as set out in the General Data Protection Regulations (GDPR) which are in force from 25 May 2018:

## **The Principles of Data Protection**

GDPR requires that anyone processing personal data must comply with the following principles:

- Personal data must be fairly and lawfully processed
- Personal data must be processed for specified limited purposes
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate and up to date
- Personal data must not be held for longer than is necessary
- Personal data must be processed in line with the data subject's rights
- Personal data must be secure
- Personal data must not be transferred to other countries without adequate protection

Personal data is defined as data relating to a living individual who can be identified from:

- that data or
- that data and other information which is in the possession of; or is likely to come into the possession of. (This includes expressions of opinion about the individual).

Sensitive personal data is defined as personal data consisting of information as to:

- racial or ethnic origin
- political opinion
- religious or other beliefs
- trade union membership
- physical or mental health or condition

- sexual life
- criminal proceedings or convictions

### **Complying with the Principles of Data Protection**

HOH will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the collection and use of personal data
- Meet its legal obligations to specify the purpose for which information is used
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply checks to determine the length of time information is held
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal data is not transferred abroad without suitable safeguards
- Ensure that the rights of people about whom the information (data subjects) is held can be fully exercised under GDPR

### **The Rights of Data Subjects**

- The right to be informed that processing is being undertaken
- The right of access to one's personal data and have a free copy of the data held
- The right to prevent processing (in certain circumstances)
- The right to correct, rectify, block or erase inaccurate information without undue delay
- The right to be forgotten (in certain circumstances)

### **Our Guarantees:**

- There will always be someone with specific responsibility for data protection in the organisation
- Everyone processing personal data will understand their responsibilities under GDPR
- Everyone managing and handling personal data will have appropriate training to manage their responsibilities under GDPR
- Anyone wanting to make enquiries about handling personal data, whether a member of staff or volunteer or a member of the public, will have access to clear information
- Data subjects who no longer want HOH to hold their details are enabled to make their "opt out" request in a way that is as easy as it was to provide their details
- We make no presumption of automatic consent across data gathering platforms
- Queries about handling personal data will be promptly and courteously dealt with
- Methods of handling personal data will be regularly assessed and evaluated
- Data sharing with third party organisations is limited to that necessary by the third party organisation in the carrying out of its functions
- We have made appropriate enquiries with third party organisations that they handle personal data in line with GDPR

### **Disclosure and Barring Service**

HOH will, on occasion, require staff and volunteers to undergo a DBS check in relation to specific planned work with children and or vulnerable adults or other work which may require a DBS check

HOH will comply with its obligations under the General Data Protection Regulation (GDPR), Data Protection Act 2018 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information.

### **Storage and Access**

Any DBS Certificate information is kept securely, using an credited online service with access strictly controlled and limited to those who are entitled to see it as part of their duties. Should paper DBS certificates be obtained, they will be stored in lockable, non-portable, storage containers with access limited to named staff.

### **Handling**

In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

### **Usage**

Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

### **Retention**

Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

Throughout this time, the usual conditions regarding the safe storage and strictly controlled access apply.

### **Disposal**

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

### **Applying the Data Protection Policy**

All HOH trustees, employees and volunteers will be made aware of HOH data protection policy and of their duties and responsibilities within it.

## **Protecting Data from unauthorised use, loss or unlawful disclosure**

In order to protect data from unauthorised use, loss or unlawful disclosure HOH will:

- Keep paper files and other records or documents containing personal / sensitive data are kept in a secure environment such as a locked filing cabinet.
- Ensure personal data held on computers and computer systems, including “cloud” systems is protected by the use of secure passwords/ encryption.
- Computers and devices will be “locked” when not in use.
- Individual passwords are such that they are not easily compromised.
- Data sent by email is protected by the use of secure servers, and by encrypted or password protected documents as appropriate.

## **Review and Audit of Policy**

The policy will be reviewed annually, usually in the first quarter of the financial year. The review will ensure that the policy is still fit for purpose and will include a review of data audit and documentation.

### **The policy will be reviewed sooner**

- **If there is an actual or potential data breach**
- **If there is a change in legislation which mean that the policy should be reviewed.**

## **Training**

All staff, volunteers and board members will be given training, appropriate to the work they are doing to ensure they are able to comply with the GDPR policy.

## **Registration with Information Commissioners Office (ICO)**

Heart of Hastings has voluntarily registered with the ICO

## **Data Protection Officer**

HOH is not required to appoint a Data Protection Officer, but has voluntarily chosen to do so, the officer is:

James Leathers, Executive Director, is Heart of Hastings CLT Limited’s Data Protection Office.

Actual or suspected data breaches should be reported immediately to him, or Shelley Feldman, Administrator, in James’s absence.

Non-urgent queries and subject access requests should be made to Shelley Feldman, Administrator.

James            [james@heartofhastings.org.uk](mailto:james@heartofhastings.org.uk)  
Shelley         [shelley@heartofhastings.org.uk](mailto:shelley@heartofhastings.org.uk) / 01424 235901

Heart of Hastings, 49-51 Cambridge Road, Hastings, East Sussex, TN34 1DT