



## Data Protection & GDPR Policy

### Introduction

Harlesden Neighbourhood Forum (HNF) is committed to protecting the rights and privacy of individuals. HNF needs to collect and use certain types of data to carry out our work. This personal information must be collected and dealt with appropriately.

The General Data Protection Regulation (GDPR) governs the use of information about people (personal data). Personal data can be held on computer or in a manual file, and includes email, minutes of meetings, and photographs. HNF will remain the Data Controller for the information held. HNF staff and volunteers will be personally responsible for processing and using personal information in accordance with the GDPR.

Trustees, staff, members and volunteers running HNF who have access to personal information, and will be expected to read and comply with this policy.

### Purpose

The purpose of this policy is to set out HNF's commitment and procedures for protecting personal data. HNF regards the lawful and correct treatment of personal information as essential to fulfilling its obligations, and is committed to maintaining the confidence of those with whom we deal with.

1. We collect limited personal information of members to involve them in HNF activities.
2. We use email to contact individuals about activities and opportunities.
3. We use email to contact individuals who are part of our membership to inform them about changes to our service or events which might be of interest to them.
4. We use emails and phone numbers to contact individuals to invite them to return as volunteers and/or to work as ambassadors.
5. We collect personal information from our partners and volunteers for HNF to ensure good communication.
6. We maintain a list of people who have donated to us before, so that we can contact them to ask them to do so again.
7. We may claim gift aid on a person's donations.
8. We maintain a list of people who have explicitly told us that they do not want to be contacted by us again.
9. We maintain contact information for anyone who has volunteered for HNF so we can contact them about future volunteering opportunities.
10. We keep our volunteer, member, and partner database information up to date.

## The GDPR

In line with GDPR principles (Article 5), HNF 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)

Where 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;

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

## Type of Information Processed

Some examples of Personal Data:

- Name
- Date of birth
- Family name
- Current and previous address
- Evening/daytime/mobile telephone numbers
- Email address
- Family relationships

Some examples of Sensitive Personal data:

- Gender
- Ethnicity
- Disability
- Marital status

HNF processes the following personal information (information that allows a person to be identified):

- Volunteer and donor name, address, email, and contact number
- Partner organisation name, email address and contact number
- Member name, email address and contact number and address.
- Information required by HMRC in relation to financial donations subject to Gift Aid.

Personal information is emailed to a secure email address by the member, volunteer, partners, or donor and is then uploaded to the database. If paper requests for membership or volunteer applications are received, they are uploaded to the database upon which the paper copy is destroyed.

Staff data including personal and financial records are only available to the Chair, Treasurer, Coordinator and payroll.

Groups of people within the organisation who will process personal information are:

- Trustees, staff, specific contractors, volunteers.

## Applying GDPR within HNF

While access to personal information is limited to the trustees and staff at HNF, volunteers at HNF may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

### **Correcting data**

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them.

### **Responsibilities**

HNF is the Data Controller under the GDPR, and is legally responsible for complying with the GDPR, which means that it determines what purposes personal information held will be used for.

The Board of Trustees will consider legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
  - ✓ The right to be informed that processing is being undertaken
  - ✓ The right of access to one's personal information
  - ✓ The right to prevent processing in certain circumstances and
  - ✓ The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information

**The Data Protection Trustee on the Board of Trustees is:** Paul Anders

**The Data Protection Officer is:** HNF Coordinator

**Name:** Ilaria Esposito

**Contact Details:** [info@harlesdenneighbourhoodforum.com](mailto:info@harlesdenneighbourhoodforum.com)

The Data Protection Officer(s) will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- 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.
- Everyone processing personal information is appropriately supervised.
- Anybody wanting to make enquiries about handling personal information knows what to do.
- Dealing promptly and courteously with any enquiries about handling personal information.
- Describe clearly how HNF handles personal information.
- Will regularly review and audit the ways HNF holds, manages, and uses personal information.
- Will regularly assess and evaluate HNF methods and performance in relation to handling personal information.
- All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to 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 GDPR.

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

### **Training**

Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms:

On induction: all volunteers are given a copy of our data protection policy and asked to sign the Volunteers' Agreement to show they have read and understood it. Specific induction is given regarding volunteer roles that deal with personal data. Only staff and trustees have access to passwords and locked files.

General training / awareness raising: Before every meeting or event attended or that we support there is a reminder briefing in which the responsibilities of the volunteer and data protection are highlighted.

Further training is available to trustees and staff through outside agencies where necessary and a training log is kept of those who have attended.

## **Data collection and retention**

Before personal information is collected, we will consider:

- What information we need to deliver our work efficiently
- What information we need to show the impact of our work

We will keep data for a maximum of 5 years from the individual's last contact with us.

We will keep volunteer data for 1 year after their last contact with us, then it will be deleted.

We will keep data on Gift Aid declarations for 6 years, in accordance with HMRC regulations.

Anonymised data and aggregate totals will be maintained beyond the destruction of individual records so we can assess the impact of our services.

Application forms, interview records (including notes taken at interview) and references for unsuccessful internal or external candidates for paid employment will be kept for a period of 12 months following application, after which they will be shredded.

Once an employee has left any information relating to them held by their line manager should be handed over to the Coordinator or the Board of Trustees.

6 years after employees have left, all information other than their name, job title, department and period of employment will be deleted.

Data relating to disciplinary and grievance records of current employees are removed from personnel files once they become spent in accordance with HNF disciplinary procedure; and deleted three years from the date issued. Where disciplinary or grievance cases have involved concerns of sufficient severity or gravity, data will be deleted five years from the date issued.

We will inform people whose information is gathered about the following:

- That we need key information to deliver our work.
- That their information will be recorded in our database, which is only accessed by staff and trustees and is password protected.
- That by ticking the box on the membership and/or volunteer form, they consent to HNF using their anonymised data.
- That by ticking the box on the membership and/or volunteer form, they can opt into our communications about future events, etc.
- That by ticking the box on the membership form, they consent to being contacted for us to involve them in the HNF work.

- That donors will need to explicitly opt into our communications, including requests for further donations.
- That staff will have relevant financial and personal information kept in the HR files to enable HNF to meet legal and contractual obligations.

### **Data Security**

Once received, all correspondence containing ‘personal’ or ‘sensitive personal’ data must immediately be either securely processed, stored, or destroyed; or immediately passed on to another member of staff or a volunteer for secure processing, storing or destruction.

#### **No visible, unattended data**

All staff and volunteers must adopt a ‘clear desk policy’ when it comes to data. This means that all versions of any ‘personal’ or ‘sensitive personal’ data must be handled in a timely and secure fashion and at no time left unattended, particularly outside hours of business e.g. not left on desks overnight.

#### **Electronic copies**

Electronic copies should at no time left open and unattended on a computer monitor, and never should be unnecessarily distributed.

Computer screens should be locked if they are left unattended for any time.

All electronic correspondence containing ‘personal’ or ‘sensitive personal’ data should be deleted, and then deleted from any electronic ‘trash’ bin once it has been processed.

#### **Paper copies**

Paper copies should exist in only one of three states; being securely processed, being securely stored, or being securely destroyed.

The organisation will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure. The following measures will be taken:

All forms are emailed to a secure email address which only staff members and two trustees have access to.

Volunteers are sometimes required to collect the above data from Members and record on a paper form. All volunteers are specifically told in their induction and reminded at each session briefing that all paper copies should be given to the Coordinator at the end of each meeting or event.

All volunteer and partner information are contained on separate, password protected spreadsheets.

Any paper copies of volunteer agreements are kept in a secure filing cabinet.

A record of the DBS numbers registered.

HNF will use our best efforts to ensure that any outside agencies or contractors used to process data (such as payroll and fundraising) also comply with the law and will adhere to the GDPR regulations.

### **Existing Records**

HNF intends to use the “legitimate interest” principle of the GDPR in relation to information about volunteers and donors which was collected and stored before the date of this policy. Appendix 1 details the circumstances in which legitimate interest will be applied.

### **Data Breach**

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action being taken.

The trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

If a volunteer or member of staff is made aware of a data breach, they should notify the HNF Coordinator.

Any serious data breaches or data loss will be reported to the Information Commissioner’s Office and the Charity Commission. This includes:

- Charity data that has been accessed by an unknown person and/or deleted.
- A charity device, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police.
- Charity funds lost due to an online or telephone ‘phishing scam’, where trustees were conned into giving out bank account details.
- A Data Protection Act breach has occurred and been reported to the ICO.
- Data Subject Access Requests

Anyone whose personal information we process has the right to know

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to HNF at ([info@harlesdenneighbourhoodforum.com](mailto:info@harlesdenneighbourhoodforum.com)) or verbally.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- Relationship with the organisation and applicable timescales

We may also require proof of identity before access is granted. The following forms of ID may be required: passport, birth certificate.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 28 days required by the GDPR from receiving the written request.

### **Disclosure**

HNF may need to 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 HNF to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a Data Subject or other person
- The Data Subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice, or defending any legal rights

- Monitoring for equal opportunities purposes – e.g. race, disability or religion Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. a safeguarding concern for the welfare of a child or adult

HNF regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

### **Risk Management**

The consequences of breaching Data Protection can cause harm or distress to members, volunteers and partners. Trustees, staff and volunteers should be aware that they can be held personally liable if they use personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of HNF is not damaged through inappropriate or unauthorised access and sharing.

### **Further information**

If members of the public/or stakeholders have specific questions about information security and data protection in relation to HNF please contact the Coordinator.

The Information Commissioner's website ([www.ico.gov.uk](http://www.ico.gov.uk)) is another source of useful information.

## **Appendix 1: HNF GDPR Approaches**

### **Background and Definitions**

#### **CONSENT**

*Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:*

*...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*

Under the GDPR, organisations using consent as the basis for contact or data processing, will need to actively collect and then maintain consents (opt-ins) from existing and new contacts in order to store information, or before any contact can be made (using personal data). The bar is set very high on the quality of this consent.

#### **LEGITIMATE INTEREST**

*GDPR presents legitimate interest as a valid condition for processing as follows:*

*"where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

Organisations using legitimate interest as the basis for processing data will need to be able to demonstrate that they have balanced the rights of the individual data subject with their own interests. They will need to record and explain the rationale for using legitimate interest and they need to be aware that the data subject can challenge.

Contacting all individuals who we already hold data on to collect permission could lead to a significant reduction in numbers of people on our databases. Not everyone will respond and of those that do, tick a consent box – even if they are actively in contact with HNF. Harvesting and maintaining permissions could quickly become the major preoccupation of operating teams.

Legitimate interest is a simpler approach and recent guidance from the Information Commissioner's Office (ICO) suggests they now consider this route is likely to be chosen by charities in many cases. However, the charity needs to specify and record the grounds on which it believes legitimate interest applies in each case. Organisations can also not rely on consent and legitimate interest for the same set of data, i.e., if a group of individuals are contacted to request consent but consent is not given by some, we could not then retain their information under legitimate interest.