Hilldrop Area Community Association

Privacy Policy

July 2021

Policy No. 03	This policy was adopted by HACA in May 2018 and will be reviewed at least every 2 years.	**Date of Review:** June 2021

CONTENTS Page

1. Aim

The Hilldrop Area Community Association (HACA) needs to keep certain information on its employees, volunteers, donors, suppliers and service users to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

HACA is committed to ensuring any personal data will be dealt with in line with the 2018 General Data Protection Regulation (GDPR).

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers all staff, trustees and volunteers at HACA.

2. Definitions

For data to be classified under 'personal data' it must:

a) Be data (so not unrecorded conversations with service users, donors or customers).

b) Be personal. Data is personal if it is relating to identifiable, living individuals who:

i. can be identified or who are identifiable, directly from the information in question; or

ii. who can be indirectly identified from that information in combination with other information.

It does not matter whether this data was processed automatically, electronically or manually.

Personal data may also include **special categories of personal data** or **criminal offences data**. These are considered to be more sensitive and you may only process them in more limited circumstances.

For data to be classified as '**special category data'** it must fall into the following categories:

a) The racial or ethnic origin of the subject.
b) The subject's political opinions.
c) The subject's religious or philosophical beliefs.
d) Whether the subject is a member of a trade union.
e) Information on the subject's physical or mental health.
f) Information on the subject's sexual orientation or activity.
g) Genetic or biometric data.

Data classified as '**criminal offences data'** includes:

a) Information about the subject's criminal activity, allegations, investigations and proceedings.
b) Any other personal data relating to the subject's criminal convictions and offences including unproven allegations; information relating to the absence of convictions; and personal data of victims and witnesses of crime.

c) Security measures relating to the subject, including personal data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.

3. Responsibilities

Overall responsibility for personal data rests with the governing body. In the case of HACA, this is the Board of Trustees. The trustees delegate tasks to the Data Protection Lead. They are responsible for:

a) understanding and communicating obligations
b) identifying potential problem areas or risks
c) producing clear and effective procedures
d) notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

All staff and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary action.

4. Notification to the Information Commissioner

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

5. Principles

HACA will use the following principles with regards to personal data. 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.
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.
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.

Valid reasons for processing data include:

a) The individual whom the personal data is about has consented to the processing.
b) The processing is necessary in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
c) The processing is necessary because of a legal obligation.
d) The processing is necessary to protect the individual's "vital interests".

e) The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
f) The processing is in accordance with the "legitimate interests" condition.

6. Types of information processed

An information audit reveals that HACA processes the following personal information:

Type of information	Details
Job applicants	Contact details; application forms & CVs; equal opportunities monitoring data; criminal offences data.
Employee information	Contact details; contractual information; qualifications, training & professional development data; health declaration data; financial data; salary and pension records.
Trustee information	Contact details; next of kin details; qualifications, training & professional development data; declaration of interest data; equal opportunities monitoring data; criminal offences data.
Volunteer information	Contact details; next of kin details; application forms & CVs; equal opportunities monitoring data; criminal offences data;
Service User information	Contact details; equal opportunities monitoring data; registration forms; detailed case notes; website/social media user statistics (anonymised).
Donor information	Contact details; donation details (financial or in-kind).
Partner information	Contact details; payment details
Supplier information	Contact details; payment details.
Visual data via CCTV	Arrival & departure of staff, service users & hirers; presence and behaviour of members of the public; vehicle registration numbers.

CCTV

CCTV is used for maintaining the security of property and premises and for preventing and investigating crime. It may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required this information may be shared with the data subjects themselves, employees and agents, service providers, police forces, security organisations and other relevant enquirers.

7. Data register

The Data Protection Lead will maintain an up-to-date data register that provides details on personal data processed by HACA, why it is being processed, the categories of individuals and categories of personal data and retention schedules.

Lawful basis for processing

The data register will state the lawful basis for the processing of personal data.

Where information is processed in accordance with the consent of the individual we will require properly documented, subject specific, granular, clear, prominent opt-ins which can be easily withdrawn.

Where information is processed in accordance with the Legitimate Purposes of the organisation, we will complete a Legitimate Interest Assessment (LIA). This comprises three steps:

a) The assessment of whether a legitimate interest exists;
b) The establishment of the necessity of processing; and
c) Undertaking a balance of interests test.

Children under 16 cannot give consent. We will seek consent from a parent or guardian and will verify that the person giving consent on behalf of a child is allowed to do so.

8. Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

The following measures will be taken:

a) Using lockable cupboards (with restricted access to keys)
b) Password protection on personal information files
c) Setting up computer systems to allow restricted access to certain areas
d) Back up of data on computers (onto a server/the cloud off site)
e) Expired or no longer relevant data will be safely disposed of by full deletion from computers, database software, cloud services, back up servers or devices, and shredding of paper documentation.

Sensitive personal information will be stored using additional security measures and will never be shared over email.

9. Data Processing Suppliers

If HACA decides to use an organisation to process data on our behalf we will:

a) Select a reputable organisation offering suitable guarantees as to their ability to ensure the security of personal data.
b) Ensure the organisation has appropriate data security measures in place.
c) Ensure the processor makes and has made appropriate security checks on its staff.
d) Ensure the contract is enforceable in the UK
e) Require the processor to report any security breaches or other problems (including requests for personal data)
f) Have procedures in place to allow HACA to act appropriately on receipt of security or problem reports from the processor.

10. Data protection by design

We will carry out a Data Protection Impact Assessment (DPIA) when:

a) Using new technologies; or
b) Processing is likely to result in a high risk to the rights and freedoms of individuals, for example large scale, systematic monitoring of public areas (CCTV).

Each DPIA will contain:

a) A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
b) An assessment of the necessity and proportionality of the processing in relation to the purpose.
c) An assessment of the risks to individuals.
d) The measures in place to address risk, including security and to demonstrate that how we comply.

11. Employee & volunteer responsibilities

All employees and volunteers are required to read and understand HACA's policies relating to privacy and data protection and are made aware of their personal liabilities and the liabilities of HACA under the GDPR. Employees and volunteers are informed of the possibility that they may commit a criminal offence if they deliberately try to access, or to disclose, information without authority, and they will also be subject to disciplinary procedures, including dismissal where appropriate.

12. Procedure for assisting the authority in responding to Freedom of Information requests

We will not provide personal information to private companies or government bodies other than that which we may be legally required to provide. We are required to share information outside the service in the rare event that we think that an adult or child is at imminent risk of significant harm, as defined under our Child Protection and Safeguarding Adults Policies.

Statutory authorities and other public bodies are required to respond to requests under the Freedom of Information (FOI) Act 2000. In some cases HACA may hold relevant information and be approached by the statutory authority for information.

The HACA will require full details from the statutory authority about the nature of the request and the information required, in order to make a decision about whether or not HACA is willing to provide the information.

Requests should be made by the statutory authority to the Head Of Centre. Decisons about whether or not to disclose will be made within 3 working days and the relevant information passed on (if appropriate) within 10 working days of the request being made.

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

13. Procedure in case of a breach

When a breach of data protection occurs The Data Protection lead will report the breach to the Information Commissioner within 72 hours and/or to any partners with which we hold Information Sharing or Partnership Agreements

If a breach is likely to result in a high risk (e.g. criminal activity such as fraud, or published in the public domain) to the rights and freedoms of individuals then the Data Protection lead will also notify those concerned and the Charity Commission.

14. Subject access requests and individual rights

Anyone whose personal information we process has the following rights:

a) The right to be informed.
b) The right of access.
c) The right of rectification.
d) The right to erasure.
e) The right to restrict processing.
f) The right to data portability.
g) The right to object.
h) The right not to be subject to automated decision making including profiling.

Any person wishing to exercise the right of access should apply in writing to the Administrator at HACA.

We may make a charge of £10 on each occasion access is requested.

The following information will be required before access is granted:

a) Full name and contact details of the person making the request.
b) Their relationship with the organisation.

We may also require proof of identity before access is granted.

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 and will ensure it is provided within a month of receiving the written request and relevant fee. Information will be presented in clear and plain language, in an intelligible and accessible form.