HARC
Homeless & Rootless at Christmas
SHEFFIELD

HARC DATA PROTECTION POLICY WITH GDPR

AND PROCEDURES

Introduction

HARC is a Data Controller under the Data Protection Act and the General Directive on Data Protection (GDPR), which means that it determines the purposes for which personal information will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

HARC needs to keep certain information about its employees, service users and volunteers to allow it to monitor its performance, achievements and operate effectively. It is also necessary to process information so that staff can be recruited and paid, courses can be organised and various legal obligations to funding bodies and government complied with.

To comply with legislation, information must be collected and used fairly, stored securely and not disclosed to any person unlawfully. To do this, HARC must comply with the principles set out in the Data Protection Act 1998 and the 2018 General Directive on Data Protection(GDPR). HARC is also committed to meeting its legal requirements under the Freedom of Information Act 2000.

Information that is already in the public domain is exempt from the 1998 Act and GDPR.

The policy also applies to provision delivered in partnership with other providers and for all service users/ learners/volunteers who receive training in the HARC name.

Amendments to this policy will be made in the light of new requirements under the General Data Protection Regulation (GDPR) being introduced from May 2018.

Policy Statement

HARC will ensure that all personal data is processed fairly and lawfully, including under the new requirements of GDPR.

Any member of staff, volunteer or service user who considers that this policy has not been followed in respect of personal data about themselves, should raise the matter with the appointed Data Protection Controllers initially. HARC has a nominated Data Protection Officer,

Procedure

Data Held and Processed

All staff, volunteers or service users and others are entitled to-

- Know what information HARC holds and processes about them, and why

- Know how to gain access to it
- Know how to keep it up to date
- Know what HARC is doing to comply with its obligations under the 1998 and 2000 Acts as well as GDPR

Personal Data

- Must be fairly and lawfully processed
- Must only be obtained for specified and lawful purposes
- Must be adequate, relevant and not excessive in relation to the purpose for which it is required
- Must be accurate and, where necessary, kept up to date
- Must only be processed and kept for as long as is necessary
- Must be processed in accordance with the data subject's rights under the Act
- Must be protected against unlawful processing, accidental loss and destruction or damage
- Must not be transferred to a country or territory outside the EEC, unless adequate levels of protection/freedoms are in place.

Accordingly, under GDPR, Personal Data we process should be:

1. Lawful, fair and transparent
2. Limited for its purpose
3. Adequate and necessary
4. Accurate
5. Kept only for as long as needed
6. Provide for Integrity and Confidentiality

Data Protection Controller

HARC has a designated Data Protection Controller (Liz Grasso) General Data Protection Regulation (from 2018)

Initial preparation under the new regulation will include the following:

a) Awareness raising for key managers and staff within HARC to understanding the impact of the legislation and compliance requirements

b) Documenting personal information that is held by HARC including its source and where it is shared through an information audit, noting the legal basis for collection and processing
c) Making amendments to the information we give to staff and service users about how we will use their information (privacy notice) and how long it will be retained
d) Review HARC processes for deleting personal data and electronic records including direct marketing implications
e) Review how HARC responds to subject access requests within new reduced time limits
f) Review how consent is obtained and recorded with an effective audit trail
g) Review procedures for detecting, reporting and investigating personal data breach
h) Implement a process to carry out Privacy Impact Assessments in high risk situations
i) Review the role of Data Protection Officer in the organisation

The Data Protection Act Legislation

This contains 8 principles for processing personal data with which HARC will comply. Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s)

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller, who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information HARC will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998

Data Subject/Service User – The individual whose personal information is being held or processed by HARC (for example: a service user or a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

(a) Racial or ethnic origin of the data subject
(b) Political opinions
(c) Religious beliefs or other beliefs of a similar nature
(d) Trade union membership
(e) Physical or mental health or condition
(f) Sexual orientation
(g) Criminal record
(h) Proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioner's Office (ICO) about the data processing activities of HARC. Note: Not-for-profit organisations are exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of HARC.

Applying the Data Protection Act within the HARC

Whilst access to personal information is limited to the staff and volunteers at HARC, Volunteers at HARC 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

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

The management committee 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 fulfill 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 Act. 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 Officer on the management committee is:

Name : Liz Grasso

Contact Details: 07523 927318

The Data Protection Officer 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 it handles personal information
- Will regularly review and audit the ways it holds, manage and use personal information
- Will regularly assess and evaluate its 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 Data Protection Act 1998.

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

Data collection

Informed consent

Informed consent is when

- A Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- And then gives their consent.

HARC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, HARC will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing

- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is HARC's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

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 Data Protection Act 1998.

Data Subject Access Requests

Members of the public may request certain information from the Local Authority under the **Freedom of Information Act 2000**. The Act does not apply to HARC. However, if at anytime we undertake the delivery of services under contracts with the Local Authority we may be required to assist them to meet the Freedom of Information Act request where we hold information on their behalf.

Disclosure

HARC 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 HARC 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.

HARC 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.

HARC intends to ensure that personal information is treated lawfully and correctly.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they could be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of HARC is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data.

Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of administering the campaign/project and securely dispose of once the promotion and monitoring period is complete. If a customer is housebound and receives regular visits from a volunteer – ensure the list is securely stored and remove customer details when they change or the customer no longer receives the service. Review the list annually. We will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to the [Group] please contact the Data Protection Officer:

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.

Signed: Julie Roberts (Chair)

Dated: 14/09/23

Reviewed JR - 14th September 2023