Hainworth Wood Community Centre

Data Protection Policy

Policy statement

As an organisation we need to collect and use certain types of information about the different people we come into contact with in order to carry out our work. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material. This policy applies to all personal and sensitive personal data. We will:

- comply with the General Data Protection Regulations in respect of the data we hold about individuals;
- respect individuals' rights
- be open and honest with individuals whose data is held;
- ensure that everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- protect the organisation's service users, employees, volunteers and other individuals;
- provide training, support and supervision for employees and volunteers who handle personal data, so that they can act legally, confidently and consistently;
- regularly assess and evaluate our methods and performance in relation to handling personal information; and
- protect the organisation from the consequences of a breach of its responsibilities.

We recognise that our first priority under the General Data Protection Regulations is to avoid causing harm to individuals. Information about employees, volunteers and service users will be used fairly, securely and will not be disclosed to any person unlawfully.

Secondly, the Regulations aim to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, we will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

*Personal data is any information about a living individual which allows them to be identified (for example a name, photographs, videos, email address or address). Identification can be by the information alone or in conjunction with other information.

This policy applies to all our employees, trustees and volunteers.

Data Privacy Principles

- All personal data will be processed lawfully, fairly and in a transparent manner;
- Personal data will only be collected for the specified, purposes outlined within "What information we collect about you" and will not be further processed in a manner that is incompatible with those purposes.
- Personal data that we collect will be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. The information which we collect is outlined in the section below "What information we collect about you".
- We will take all reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.
- Personal data will be kept in a form that permits identification for no longer than is necessary for the purposes for which the personal data has been collected for processing, in line with the HWCC Retention Policy.
- We will hold and process personal data in a manner that ensures appropriate security. We outline this in the "Keeping your information safe" section of this policy.

Disclosure

We may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware of how and with whom their information will be shared. There are circumstances where the law allows us as an organisation to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Processing carried out by individuals purely for personal or household activities including correspondence and the holding of addresses or social networking and online activity undertaken within the context of these activities;
2. Processing covered by the Law Enforcement Directive;
3. Processing for national security.

We regard 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.

Data Controller

Hainworth Wood Community Centre is the Data Controller under the Act, which means that it determines what purposes personal information held, 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.

Responsibilities

The Trustees recognise their overall responsibility for ensuring that **Hainworth Wood Community Centre** complies with its legal obligations.

The Data Protection Officer has the following responsibilities:

- Briefing the Board on Data Protection responsibilities;
- Reviewing Data Protection and related policies;
- Ensuring that Data Protection induction and training takes place;
- Handling subject access requests;
- Approving unusual or controversial disclosures of personal data;
- Ensuring contracts with Data Processors have appropriate data protection clauses;
- Electronic security;
- Ensuring that all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been disposed of or passed on/sold to a third party.
- Approving data protection-related statements on publicity materials and letters

Each employee, trustee and volunteer who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed. All employees, trustees and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under our disciplinary procedures.

Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, we have a separate Confidentiality Policy. This Data Protection Policy should be read in conjunction with the Confidentiality Policy.

In order to provide some services, we will need to share client's personal data with other agencies (Third Parties). Verbal or written consent will always be sought from the client before data is shared.

Where anyone within the organisation feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure

request is received, this will only be done after discussions with the Data Protection Officer and/ or Chair. All such disclosures will be documented.

Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information on clients, volunteers and employees will be:

- Kept in locked cabinets (paper), on a password protected computer in the office or on the cloud (password protected)
- Protected by the use of passwords if kept on computer or encrypted if appropriate
- Destroyed confidentially if it is no longer needed, or if an individual requests

Access to information on the main database is controlled by a password and only those needing access are given the password. Employees, trustees and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

Notes regarding personal data of clients should be shredded or destroyed.

Data recording and storage

We have a single database holding basic contact information about all clients and volunteers. The back-up copies of data are kept in a locked cabinet or on the cloud.

We will regularly review our procedures for ensuring that our records remain accurate and consistent and, in particular:

- We will keep records of how and when information was collected.
- The database system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in a single place, and all employees, trustees and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Effective procedures are also in place to address requests from data subjects for access to, amendments or the erasure of their information
- Employees, trustees and volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping in compliance with the GDPR.
- Data will be corrected if shown to be inaccurate.

We store archived paper records of clients and volunteers securely in the office.

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

Access to data

Information and records will be stored securely and will only be accessible to authorised employees, trustees and volunteers, and the individual to whom the information relates.

All users and volunteers have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.

Subject access requests must be in writing or by email. All employees, trustees and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay. In accordance with the GDPR, we will provide personal data in a 'commonly used and machine readable format.' We also recognise the right of the individual to transfer this information to another Controller.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

We will provide details of information to service users who request it unless the information may cause harm to another person.

Employees have the right to access their file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify the Data Protection Officer or Chair so that this can be recorded on file.

Transparency

We are committed to ensuring that in principle Data Subjects are aware that their data is being processed and:

- for what purpose it is being processed;
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Employees: in the staff terms and conditions
- Volunteers: in the volunteer welcome/induction pack
- Trustees: in the roles and responsibilities/induction pack
- Users: when they provide their information and consent to retain it is requested, or when they request (on paper, online or by phone) services

Standard statements will be provided to all staff for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

Consent

Staff details will only be disclosed for purposes unrelated to their work for the organisation (e.g. financial references) with their consent.

Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about users will only be made public with their explicit consent. (This includes photographs.)

Consent will be obtained from parents, if children's data is being stored or processed depending on the age of the child/young person in accordance with legislation.

'Sensitive' data about clients (including health information) will be held only with the knowledge and consent of the individual.

Consent should be given in writing, although for some services it is not always practicable to do so. In these cases verbal consent will always be sought to the storing and processing of data, and records kept of the dates, and circumstances. Online consent will be requested when clients sign up to services, donate or sign up to mailing lists. In all cases it will be documented on the database that consent has been given.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing (see below).

We acknowledge that, once given, consent can be withdrawn by the Data Subject at any time. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct marketing

We will treat the following unsolicited direct communication with individuals as marketing:

- seeking donations and other financial support;
- promoting any of our services;
- promoting our events;
- promoting membership to supporters;
- promoting sponsored events and other fundraising exercises;
- marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be asked to provide their consent. We do not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Training

All employees and volunteers that have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection policy, Confidentiality policy and the operational procedures for handling personal data. All staff and volunteers will be expected to adhere to all these policies and procedures.

Data Protection will be included in trustee training and the induction training for all volunteers.

Policy review

This policy will be reviewed and updated as necessary in response to changes in relevant legislation, contractual arrangements, and good practice or in response to an identified failing in its effectiveness.

Date Policy Adopted: 21.02.2022

Policy Review Date: Sept 2022