Tel: 020 8373 6268
admin@enfieldva.org.uk
www.enfieldva.org.uk
Fax: 020 8373 6267

Enfield Voluntary Action (EVA), Community House, 311 Fore Street, Edmonton, N9 0PZ

ENFIELD VOLUNTARY ACTION
DATA PROTECTION POLICY

Contents

Introduction

This policy applies to all staff, trustees and volunteers of Enfield Voluntary Action.

The purpose of this policy is to enable Enfield Voluntary Action to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect Enfield Voluntary Action's service users, staff, volunteers and other individuals
- protect the organisation from the consequences of a breach of its responsibilities

The General Data Protection Regulation 2018

Article 5 of the GDPR requires that 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; 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;

(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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(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.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

To fulfil this clause EVA completed a data mapping exercise. This is a written working document of steps taken to prepare for GDPR and log the steps taken in reviewing practice in order to ensure compliance. This is EVA's Data Protection Preparation and Review Log, which outlines technical and organisational measures to show EVA's consideration and integration of data protection in processing activities.

Policy Statement

Enfield Voluntary Action will:

- Comply with both the law and good practice and meet any other legal requirements
- Respect individuals' rights

- Be open and honest with individuals whose data is held
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

Enfield Voluntary Action recognises that its first priority under the Data Protection Act and GDPR is to avoid causing harm to individuals. Information about staff, volunteers and service users will be used fairly, securely and not disclosed to any person unlawfully.

Secondly, the Act and GDPR 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, Enfield Voluntary Action will seek to give individuals as much choice and clarity as is possible and reasonable over what data is held and how it is used.

EVA strives to conduct all activities with data protection by design and default to respect the privacy of individuals, service users, staff, trustees and volunteers.

Definitions

Personal Data
Personal Data is any information that can identify a person. Pseudonymisation and anonymised is not applicable to GDPR because the information cannot be identified.

Organisation Data
The Privacy and Electronic Communications Regulation (PECR) states that organisation contact details in the public domain is not subject to GDPR.

This means that if a contact from an organisation provides EVA with a contact detail such as a phone number, address or email address in matters relating to their organisation, EVA will assume these contact details are organisational details and therefore not subject to GDPR. However, EVA has a policy not to pass any contact details to any third parties if the contact details are not in the public domain (usually from checking the organisation's website or the Charity Commission website).

Organisation data is different to the data of individuals, such as the volunteers or parents that access EVA services outside the identity of an organisational structure. GDPR applies to these individuals and therefore EVA treats such individuals as data subjects with the full range of rights under GDPR.

Data Subject
The Data Subject is the individual whose personal data is being processed. Examples include:

- employees – current and past
- volunteers
- job applicants
- donors
- users
- suppliers

Data Controller

The Data Controller is the legal 'person' within EVA that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act and GDPR and is the Chief Executive of EVA.

Data Processor

EVA is the Data Processor in most processing activities as the majority of data is processed internally. However, EVA sometimes instructs other organisations to process data on EVA's behalf, in which case EVA will have a written contract and discuss GDPR to check the following (APPENDIX 4):

- What happens after data is transferred from EVA to the third party?
- Whether staff within the external Data Process are trained?
- What happens to data once the task is complete? I.e. what is the retention policy of the external Data Processor?

Information Asset Owner (IAO)

In EVA, the Chief Executive is the Information Asset Owner, as this position is responsible for identifying data assets.

Senior Information Risk Owner (SIRO)

EVA will appoint a Data Protection Officer from board members to fulfil the role of Senior Information Risk Owner, as this position requires a person at board level who is responsible for setting organisation policies.

Lawful Processing

Processing data for EVA means:

- obtaining and retrieving
- holding and storing
- making available within or outside the organisation
- printing, sorting, matching, comparing, destroying.

Under the GDPR there are 6 main lawful processing conditions:

1. Consent
2. Necessary for contract
3. Legal obligation
4. Vital interests
5. Lawful Authority
6. Legitimate interests

Principles of Processing

When processing data EVA will consider the following principles:

1. Fair, lawful and transparent – How is the data used?
2. Compatible and specific – What is the purpose of the data?
3. Relevant and limited – Is the data necessary?
4. Rectifiable – Is the data accurate?
5. Retaining for no longer than necessary – How long is the data needed?
6. Integrity and confidentiality – Is the data secure?

Consent

Consent must be freely given and in the form of a positive opt-in, for example, consent for EVANews will be collected through an opt in of email addresses on EVA's website.

Consent under GDPR must be transparent and therefore:

- Specific
- Clear
- Prominent
- Informed
- Opt-in
- Properly documented
- Easily withdrawn

Written consent is always preferable, but in some cases it may be necessary for verbal consent or implied consent. For example, if an individual has attended a course and a similar course is organised and the individual is contacted about the new course. In this case implied consent could be used.

If implied consent cannot be used, the individual may be phoned, unless the person is registered on the telephone preference service or written to. If EVA requires a telephone number, they may be able to check with a telephone preference cleaner service, which can be found at the following address;

https://corporate.tpsonline.org.uk/index.php/tps/cleaners

If anyone other than parents are bringing a child to the creche or are providing any personal details about the child, parental consent will be required.

Individual Rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

1. **The right to be informed**
   EVA will fulfil this responsibility through privacy notices, which must be concise, intelligible, easily accessible and written in clear plain English.

2. **The right of access**

EVA will provide information about personal data, which must be free unless excessive, and within 1 month unless complex.

3. **The right to rectification**
   EVA will respect the right to rectification when personal data is inaccurate or incomplete and the response should be within 1 month unless complex.

4. **The right to erasure**
   EVA will erase personal data where it no longer necessary for its original purposes; where consent is withdrawn; to comply with a legal obligation; or is found to have been collected unlawfully. This is also known as the 'right to be forgotten'.

5. **The right to restrict processing**
   EVA will restrict processing where an individual data subject contests the accuracy of the personal data or an individual objects to the processing.

6. **The right to data portability**
   Data portability is not currently applicable to EVA's services.

7. **The right to object**
   EVA respects a data subject's objective to processing data or direct marketing and this right should be included in EVA's privacy statement.

8. **Rights in relation to automated decision making and profiling**
   Data subjects have the right to not be subject to a decision when it is based on automated processing; and obtain human intervention, express their views, obtain an explanation and challenge the decision.

Responsibilities and Promoting Accountability and Governance

The Board of Trustees recognises its overall responsibility for ensuring that Enfield Voluntary Action complies with its legal obligations and recognises the importance of promoting accountability and governance.

The Chief Executive is the Data Controller and the Data Asset Owner, who is responsible for deciding why and how personal data is processed internally; and identifying data assets. This role includes the following:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- 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 (if appointed)
- Electronic security
- Approving data protection-related statements on publicity materials and letters

Each member of staff and volunteer at Enfield Voluntary Action 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 staff 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.

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

Enfield Voluntary Action will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

Data Protection Impact Assessments

Data Protection Impact Assessments should be carried out if data will be used in a new way, for example when there are:

- new projects
- changes to services
- new technology is introduced

Data Protection Impact Assessments will be conducted in 5 stages:

1. Identify target
2. Assess threat
3. Assess weakness
4. Consider risk appetite
5. Implement controls

Transparency and Privacy Statements

Enfield Voluntary Action is 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:

- Staff: in the staff terms and conditions
- Volunteers: in the volunteer welcome/support pack
- Service users: when they request (on paper, on line or by phone) services

Privacy statements will be provided to data subjects where data is collected. EVA will have different notices for different groups (see Appendix 3).

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.

Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, Enfield Voluntary Action has a separate Confidentiality Policy. This Data Protection Policy should be read in conjunction with Enfield Voluntary Action's Confidentiality Policy.

Enfield Voluntary Action has a privacy statement for service users, setting out how their information will be used. This is available on request, and a version of this statement will also be used on the Enfield Voluntary Action web site. (See Appendix 3).

Staff, volunteers and sessional workers are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Confidentiality Policy and Statement.)

In order to provide some services, Enfield Voluntary Action may need to share organisations' data with other agencies (Third Parties). Verbal or written agreement will always be sought from the service users before data is shared.

Where anyone within Enfield Voluntary Action 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 a manager. All such disclosures will be documented.

Security, Data Recording and Storage

- **Staff will be encouraged to keep desks tidy and keep any recorded** information on service users, volunteers and staff will be:

  - Kept in locked cabinets
  - Protected by the use of passwords if kept on computer
  - Destroyed confidentially if it is no longer needed

- Staff should not email work with any personal data to personal email accounts
- Staff should not take any personal details away from the office unless necessary, e.g. for a specific meeting, in which case staff should be extra vigilant, and where possible transport electronic rather than paper copies.
- Devices with such electronic information should be password protected
- No personal data should be used where public wifi is being used
- Cloud based data should be based in the EU, which complies with GDPR
- No personal data should be stored on EVA tablets
- Photos from tablets should be copied to EVA office computers as soon as possible after taking them

Access to information on the main database is controlled by a password and only those needing access are given the password. Staff 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.

Enfield Voluntary Action holds basic information about all service user organisations and registered volunteers on:

- Do-It (Online Customer Relationship Management System (CRM))
- Aims (Networked CRM System)
- Training and Membership Databases (Access)

Enfield Voluntary Action will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- The database systems are regularly reviewed to encourage and facilitate the entry of accurate data and ensure a high quality of data management.
- Data on any individual will be held in as few places as necessary, and all staff 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.
- Staff and volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
- Data will be corrected if shown to be inaccurate

Enfield Voluntary Action holds both paper and computerised personal details of Staff and Volunteers. Paper copies are stored in a locked filing cabinet and computerised information is password protected.

Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

All data breaches must be notified to the ICO within 72 hours. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the individual must be notified directly.

The Data Protection Officer may communicate with an advisory body, such as ClearComms prior to reporting directly to the ICO.

Access to data

All service users 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. All staff and volunteers are required to pass on anything which might be a subject access request to the Chief Executive without delay.

All those making a subject access request will be asked to identify any other individuals who may also hold information about them, so that this data can be retrieved.

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

Staff 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 Chief Executive so that this can be recorded on file.

Direct marketing

Enfield Voluntary Action will treat the following unsolicited direct communication with individuals as marketing:

- seeking donations and other financial support;
- promoting any Enfield Voluntary Action services;
- marketing the products of Enfield Voluntary Action;
- 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 with the opportunity for the data subject to clearly opt in. The data subject will also be given a clear opt out. Enfield Voluntary Action does not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

Enfield Voluntary Action will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the Telephone Preference Service.

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

Policy review

The policy will be reviewed annually by the Chief Executive and approved by the Board of Trustees. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, new cases of data breaches, clarification of regulations, good practice or in response to an identified failing in its effectiveness.

In preparation for this data protection policy, EVA has conducted a data mapping exercise and is a live document.

Reviewed: June 2020