Advising Communities

Information sheet

Data Protection Policy: A Specimen Policy for Community Organisations

Organisations have a legal duty to ensure that the way they hold and process personal information is done so in accordance with the General Data Protection Regulations. This is an example of a policy that could be adopted by a community organisation.

Red type signifies where an organisation should complete or make appropriate decisions re deletion. Please delete this statement when you have completed drafting the policy

Introduction

Insert organisation details: (name, address and where applicable registered numbers e.g. Charity, Charitable Incorporated Organisation, Company Limited by Guarantee)

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

1. The Basics of General Data Protection Regulations 2018

1. The General Data Protection Regulations (GDPR) gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. The new General Data Protection Regulation came into effect in the UK on 25 May 2018, and will replace the Data Protection Act 1998.

The Regulations work in a number of ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

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 ('accuracy');

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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order

to safeguard the rights and freedoms of the data subject ('storage limitation');

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 ('integrity and confidentiality').

2. The Data Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

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

2. 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. adequate, relevant and not excessive in relation to those purpose(s);

4. accurate and, where necessary, kept up to date;

5. not kept for longer than is necessary;

6. processed in accordance with the rights of data subjects under the GDPR;

7. 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; and

8. not 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 second area covered by the Regulations provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records. Individuals have the right to request to see their information, and to ask for their information to be amended or erased.

2. Definitions

Confidentiality: Confidential information is defined as verbal or written information, which is not meant for public or general knowledge, information that is regarded as personal by users, members, trustees, employees or volunteers.

Consent: of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a

statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Data is one piece or a combination of information that relates to a person or a 'Data Subject' that could identify them, that is stored:

a) Electronically i.e. on computer, including word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or databases, faxes and information recorded on telephone logging systems.

b) Manually i.e. records which are structured, accessible and form part of a filing system where individuals can be identified and personal data easily accessed without the need to trawl through a file.

Data concerning health: means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

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

Data Processor or Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller

Data Protection Act 1998: The UK legislation that provides a framework for responsible behaviour by those using personal information, which will be superseded by the General Data Protection Regulations on 25 May 2018.

Data Subject: any living individual whose personal data is being processed. Examples include:

- employees – current and past
- volunteers
- apprentices
- job applicants
- donors
- service users/clients
- suppliers

'Explicit' consent: is a freely given, specific and informed agreement by an individual to the processing of personal information about them, leaving nothing implied. Explicit consent is needed for processing sensitive data.

Information Commissioner is responsible for implementing and overseeing the General Data Protection Regulations

Notification: Notifying the Information Commissioner about the data processing activities of (insert name of organisation) if required, however certain activities for not for profit organisations may be exempt from notification. See 3.2

Personal data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Processing: means the use made of personal data including any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data Protection Officer or Adviser: The person(s) responsible for ensuring that we follow our data protection policy and complies with the General Data Protection Regulations

Data Protection Officer: A qualified Data Protection officer is required by some organisations depending on the number of staff and if they process sensitive data. Every organisation is advised to check their own situation on the ICO website for guidance

Data Protection Adviser. For organisations who have checked their position as advised above and are sure they do not need a qualified Data Protection Officer we recommend that a Data Protection Adviser is appointed by every organisation to support the implementation of GDPR and be a central contact point e.g. for requests for personal data or the right to be forgotten

Sensitive Data – Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person

Third Party agreements. Many organisations use third parties to store/process data such as: online payments, online forums, cloud storage facilities. There should be a third party written agreement with the other organisation to confirm they are meeting the regulations. These can sometimes be found as web based documents. The data needs to be stored on European servers to ensure they comply with GDPR

3. 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 clients/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 clients/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.

3.1. Disclosure

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

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.

3.2. Data Controller

The Board/Trustees/Management Committee (delete as appropriate) of (Insert name of organisation) is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for.

Unless the organisation is exempt from registering with the ICO (for guidance see https://ico.org.uk/for-organisations/business/) the Data Controller 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.

There are some exemptions for not for profit organisations re registering with the ICO – but not for those who have CCTV

4. Responsibilities

The Trustees/Management Committee/Board (delete as appropriate) recognises its overall responsibility for ensuring that **(insert name of organisation)** complies with its legal obligations.

The Data Protection Officer or Data Protection Adviser (delete whichever is not appropriate for your organisation) is currently **[Insert name of member of staff]**, who has the following responsibilities:

- Briefing the Trustees/Management Committee/Board (delete as appropriate) 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 Data subject access requests;
- Approving unusual or controversial disclosures of personal data;

- Ensuring signed written agreements are in place between the Data Controller and the Data Processors and these 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 and breach of personal data may be handled under our disciplinary procedures.

5. 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. Delete if you do not have a 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 our 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 a manager or the Data Protection Officer. All such disclosures will be documented.

6. 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:

- Handled, transferred, processed and stored with the up-most care and regard.
- When not being handled, transferred or processed, it will be stored in secure office facilities, locked drawers or cabinets, or secure cloud-based digital storage.
- Protected by the use of passwords if kept on computers and/or other devices and encrypted if appropriate.
- Destroyed confidentially if it is no longer needed, or if an individual requests.

Access to information on the main database or cloud based facilities (delete as appropriate) 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.

7. Data Recording and storage

We have a single database or We use secure cloud-based systems (delete as appropriate) for holding basic information about all staff, members clients and volunteers. The back-up copies of data are kept in a safe place.

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 storage system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- 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 or a request is made by a Data Subject.

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.

8. Access to data

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

All clients and customers 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 Manager so that this can be recorded on file.

9. Data breach reporting

All Staff, Trustees and volunteers are required to report any data breach to the Data Protection Officer/Data Protection Adviser (delete as appropriate) as soon as possible once they are aware it has occurred. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration,

unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed.

The Data Controller is responsible for recording and reporting any data breaches that occur across the organisation.

Less serious breaches will be recorded and listed in an appropriate place, and trends or lessons learned will be reviewed.

Serious personal data breaches will be reported by the Data Protection Officer/Data Protection Adviser (delete as appropriate) to the Board/Trustees/Management Committee (delete as appropriate) at the earliest possible time, as well as reported to the ICO within 72 hours of the breach occurring if possible, and if not, informing the ICO the reasons for any delay.

10. 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/support pack
- Trustees: in the roles and responsibilities/support pack
- Clients: 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.

11. 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 clients 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. Proof of date of birth will be obtained

'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.

12. 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.

We 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.

13. Staff training and acceptance of responsibilities

All employees 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 (delete if you do not have these policies). 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.

We will provide opportunities for all staff and volunteers as appropriate to explore Data Protection issues through training, team meetings, and supervisions.

14. 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.

In case of any queries in relation to this policy please contact our Data Protection Officer or Data Protection Adviser (delete as appropriate) : …… at: ……..
(Insert details here)

Date Policy Adopted:

Policy Review Date:

Appendix

Privacy statement

Insert organisation details here: (name, address and where applicable registered numbers e.g. Charity, Charitable Incorporated Organisation, Company Limited by Guarantee)

When you request information from us, sign up to any of our services or buy things from us, we obtain information about you. We will ask for your consent to retain this information, and make it clear what your information will be used for. This statement explains how we look after that information and what we do with it.

We have a legal duty under the General Data Protection Regulations to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally information we hold comes directly from you, as set out in our Data Protection Policy. Whenever we collect information from you, we will ask for your consent to collect this information and make it clear what the purpose of this collection is, for example; which information is required in order to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to.

We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

If you have signed up to a training event or other service, when you sign up we will ask you for consent to pass your details to the professional worker/volunteer providing that service. That worker/volunteer may hold additional information about your participation in these activities. We have an agreement in place with our professional workers/volunteers or any other agents or sub-contractors which we need to disclose your personal information to our agents or sub-contractors. They will only able to use your personal information in accordance with this agreement. In addition, we may disclose your personal information if required to do so by law, in connection with any legal proceedings or prospective legal proceedings, and in order to establish, exercise or defend our legal rights.

We would also like to contact you in future to tell you about other services we provide, to keep you informed of what we are doing and ways in which you might like to support us. You have the right to ask us not to contact you in this way and to ask us to remove the information which we hold on you. We will always aim to provide a clear method for you to consent for your information to be stored for this purpose. You can also contact us directly at any time to tell us not to send you any future marketing material or to remove your information by contacting us at:

Email:
Phone:

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you).

To obtain a copy, either ask for an application form to be sent to you, or write to our Data Protection Officer/Data Protection Adviser (delete as appropriate) at the address given above. We aim to reply as promptly as we can and, in any case, within the legal maximum of 30 days.

Updating This Statement

We may update this privacy policy by posting a new version on this website at any time. You should check this page occasionally to ensure you are familiar with any changes.

Other Websites

This website may contain links to other websites. We are not responsible for the privacy policies or practices of any third party.

The material in this document does not give a full statement of the law, nor does it reflect changes after May 2018. It is intended for guidance only and is not a substitute for professional advice. No responsibility for loss occasioned as a result of any person acting or refraining from acting on the basis of this material can be accepted by the author or by Advising Communities.

Advising Communities, The Foundry, 17 Oval Way, London, SE11 5RR
Registered Company No: 03316471, Charity No: 1061055.
Registered Office: 6-8 Westmoreland Road, London, SE17 2AX

T 0300 0301 121
E organisations@advisingcommunities.uk