Advising Communities

Data Protection Policy

Effective 25th May 2018

Introduction

Advising Communities is a registered charity in England and Wales, and a registered company limited by guarantee. Registered Charity Number 1061055. Registered Company Number 03316471. Registered at 6-8 Westmoreland Road, London, SE17 2AX

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

1. The Basics of General Data Protection Regulation

1. The General Data Protection Regulation (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 General Data Protection Regulation came into effect in the UK on 25 May 2018, and replaces the Data Protection Act 1998.

The Regulation 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;

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 or other electronic devices or digitally 'in the cloud', 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's Office (ICO): is responsible for implementing and overseeing the General Data Protection Regulations.

Notification: Notifying the Information Commissioner's Office about the data processing activities of Advising Communities, as certain activities may be exempt from notification.

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;

Sensitive Data: Data that relates to the physical, physiological, genetic, mental, economic, cultural or social identify of a person or 'Data Subject'.

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 local authorities, funding bodies and partner organisations.

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 of Advising Communities is the Data Controller, which means that it determines what purposes personal information held, will be used for. It is also responsible for ensuring that we are registered with the Information Commissioner's Office and are compliant with the GDPR.

4. Responsibilities

The Board recognises its overall responsibility for ensuring that Advising Communities complies with its legal obligations. The board delegate the day to day running of the organisation to the Chief Executive.

Advising Communities has appointed the Deputy Chief Executive as the person with responsibility for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to them.

This person also has the following responsibilities:

- Briefing the Trustee Board on Data Protection responsibilities and breaches;

- Notifying the ICO of data the organisation holds and of any significant breaches;
- Reviewing Data Protection and related policies in partnership with the SMT;
- Ensuring that Data Protection induction and training takes place for all staff and volunteers;
- Supporting the SMT in relation to subject access requests;
- Approving unusual or controversial disclosures of personal data in partnership with the CEO;
- Ensuring contracts with Data Processors have appropriate data protection clauses;
- Ensuring third party contractors are keeping our systems and data safe;

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 will be handled under our disciplinary procedures.

5. Written agreements

We treat the confidentiality of data collected and stored with the upmost importance, and we ensure comprehensive written agreements are in place between;

- the Data Controller and all data processors.
- the Data Controller and all third parties.

These written agreements ensure that anyone collecting, accessing or processing personal or sensitive information are bound to the same principals of data protection as defined within this policy.

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 stored in cloud-based facilities is controlled by a password and only those needing access are given an account and password. Employees, Trustees and volunteers should be careful about information that is displayed either physically or digitally 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 once this information has been stored digitally.

7. Data Recording and storage

We use secure cloud-based systems for holding information about staff, volunteers, Trustees and service-users. Any 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 systems are 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
- Data will be corrected if shown to be inaccurate, or if Data Subject requests.

Any archived paper records of individuals are stored securely in our office(s).

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 service users, clients and customers have the right to request access to all information stored about them. Any subject access requests will be handled by the Deputy Chief Executive within one month. In addition, they also have the right to exercise their 'rights to be forgotten', however this may be overridden by our legal obligations to hold on to data for a specified time period.

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 Deputy Chief Executive 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 Deputy Chief Executive 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

We are committed to recording and reporting any personal data breach that may occur.

All Staff, Trustees and volunteers are required to report any personal data breach to the Deputy Chief Executive as soon as possible once they are aware it has occurred. The Deputy Chief Executive is responsible for recording and reporting any data breaches that occur across the organisation.

Less serious breaches will be recorded appropriately, and trends or lessons learned will be reviewed at SMT level.

Serious personal data breaches will be reported by the Deputy Chief Executive to the Chief Executive and the Board of Trustees at the earliest possible time, as well as reported to the ICO within 72 hours of the breach occurring. If this is not possible the ICO will also be informed of the reason 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
- Service users: when they provide their information and consent to retain it as 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 related to their work for the organisation (e.g. financial references) with their consent.

Information about volunteers will be made public with their explicit consent.

Information about service 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 service users (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. All staff 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 to explore Data Protection issues through training, team meetings, and supervisions.

14. Data Protection compliance declaration

As a small organisation we collect data only on the request of those in need of advice and support, to ensure we keep a record of our advice given and to meet the requirements of those who fund our services.

We only share data externally on the expressed permission of the Data Subject to improve the support we can provide or in line with statistical and reporting requirements from our funders - and this is shared anonymously in the vast majority of cases. We have an assigned member of staff who is responsible for data protection compliance across the organisation and do not believe we meet the requirements to have a Data Protection Officer (DPO).

The Senior Management Team (SMT) work together to ensure our practices and policies are adhered to and most importantly that all of our data is kept confidentially in line with values and principles of our confidential, non-judgmental service, as well as the requirements of the GDPR.

We formally minute board decisions in this regard and we are keeping a watching brief as the GDPR comes in to force to ensure we remain up to date and compliant.

15. 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 Deputy Chief Executive (responsible for data protection compliance) at: info@advisingcommunities.uk

Date Policy Adopted:

25th May 2018

Policy Review Date:

25th May 2019

Appendix

Privacy Statement

Effective 25th May 2018

Advising Communities is a registered charity in England and Wales, and a registered company limited by guarantee. Registered Charity Number 1061055. Registered Company Number 03316471. Registered at 6-8 Westmoreland Road, London, SE17 2AX.

When you use (or request to use) any of our services, or sign up for updates from our organisation 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 Regulation 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. You do not have to provide us with any additional information unless you choose to.

We are not able to help you if you do not want us to store or process your personal information. This is because, for insurance purposes, we cannot help anyone who we cannot later identify.

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

Our services are funded by a range of different funders who ask us to share data and statistics with them as a contractual condition of funding our services. Unless otherwise stated this information will be anonymised, with all identifying information about yourself removed.

Some funders request more detailed information to be shared with them which may include personal and sensitive information about yourself. We require your permission to be able to do this and this is optional.

External auditors who check the quality of the services we provide may wish to review the help you've been given, which may also include the review of personal and sensitive information about yourself. We require your permission to be able to do this and this is optional.

We will not share your personal and sensitive information with anyone outside of Advising Communities without your recorded permission unless 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 may need to contact third parties to act on your behalf as part of the assistance you receive, we will need your recorded permission and authority in order to do this.

We ensure there are agreements in place with all data processors and third parties that may need to view, access or process your personal information. They will only be able to use your personal information in line with this agreement, and our Data Protection Policy.

If you have signed up to a training event or other service, when you sign up we will ask you for your consent to pass your details to the professional worker providing that service. That worker may then hold additional information about your participation in these activities.

You have the right to a copy of all the information we hold about you (with exception of the limited information which we may be obliged to withhold because they concern others as well as you). You also have the right to request that we change or remove the information we hold on you. Requests for us to remove information may be overridden by our legal and regulatory requirement to hold certain information on the advice we've provided for 6 years.

To request a copy of the information we hold on you, or to request we change or remove information about you that we hold, you can:

Email:

info@advisingcommunities.uk.

(Please title your email 'Data Access Request')

Write to:

Data Access Request

Advising Communities

The Foundry

17 Oval Way

London

SE11 5RR

We aim to reply as promptly as we can and we will reply 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.