**(Add name of organisation) Data Protection Policy**

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

1. **Basics of the 2018 Data Protection Act**

The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR).

The Data Protection Act[[1]](#footnote-1) states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’).
2. 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’).
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).
4. 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’).
5. 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’);
6. 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’).

The Act also provides individuals with important rights[[2]](#footnote-2), 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.

1. **Definitions**

The following words and phrases used in this Policy have the following meanings:

* ‘GDPR’ means the UK General Data Protection Regulation as applied in the UK in the 2018 Data Protection Act.

* For the purposes of this Policy, ‘data controller’, ‘data subject’, ‘personal data’, ‘processing’, ‘sharing’, ‘disclosure’ and ‘data protection principles’ shall have the meanings ascribed to them in the 2018 Data Protection Act[[3]](#footnote-3).

 For clarity:

* A **Data Controller** means the person, public authority, agency or other body which (either alone or jointly or in common with other persons) determines the purposes and means of the processing of personal data.
* **A Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
1. **Policy statement**

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

* comply with GDPR 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 priority under GDPR 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.

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.

1. **Disclosure**

We may share data with other agencies such as the local authority, funding or contracting 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:

* If a child or vulnerable adult is at risk of significant harm.
1. **Data Controller**

(Add name of organisation) 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.

1. **Responsibilities**

The Trustees/ Directors recognise their overall responsibility for ensuring that (add name of organisation) complies with its legal obligations.

The Data Protection Officer is currently (add staff name and position), who has the following responsibilities:

* Briefing the Trustees/Management Committee/Board on Data Protection responsibilities.
* Reviewing Data Protection 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;
* 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.

1. **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 clients’ 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 the Data Protection Officer. All such disclosures will be documented.

1. **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, on our secure general server or stored on our GDPR compliant CMS system (amend to reflect how data is stored securely within your organisation).
* protected with 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 and CMS 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 are shredded or destroyed.

1. **Data Recording and storage**

We have a single database holding basic information about all clients and volunteers using a GDPR compliant online CMS system (amend to reflect how data is held within your organisation).

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 as set out in our action plan, 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 in locked cabinets, or in a local secure archiving facility. At the start of every programme, we establish how long we are required to keep the data as requested by our commissioners and funders. As standard we store information for xx years unless otherwise specified.

Explicit consent is requested for photo permission. As standard we store photo imagery for xx years unless otherwise specified.

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

1. **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 the information held is inaccurate, the individual must notify their manager so that this can be recorded on file.

1. **Transparency**

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

* for what purpose it is being processed.
* what types of disclosure are likely.
* 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.

1. **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 clients, including photographs, will only be made public with their explicit consent.

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 for 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.

1. **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.

1. **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 induction training for all volunteers.

We will provide opportunities for all staff to explore Data Protection issues through training, team meetings, and supervision.

1. **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. At a minimum an automatic review will be conducted annually.

In case of any queries in relation to this policy please contact our Data Protection Officer: (add staff name and contact details).

**Appendix 1 – Definitions used in the 2018 Data Protection Act**

**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. **‘Explicit’ consent** is a freely given, specific and informed agreement by an individual to the processing of personal information about them. Explicit consent is needed for processing sensitive data.

**Data:** The GDPR definition of personal data also includes information such as name, an identification number, location data including addresses, emails, phone numbers, online identifiers including IP addresses, information gathered by cookies or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (which could include CCTV).

Data is information stored:

* Electronically i.e., on a 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.
* 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 Protection Officer:** The person(s) responsible for ensuring that we follow our data protection policy and complies with the General Data Protection Regulations.

**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 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

**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.

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

**Personal data:** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**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.

1. https://www.legislation.gov.uk/eur/2016/679/article/5 [↑](#footnote-ref-1)
2. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/ [↑](#footnote-ref-2)
3. https://www.legislation.gov.uk/eur/2016/679/article/4 [↑](#footnote-ref-3)