Project 17

St Joseph's Hospice, Mare St,
Hackney, London,

E8 4SA

www.project17.org.uk

Charity no: 1152621

Privacy and Data Protection Policy

Date created: May 2018 **Last updated: Nov 2023** **Period for review: Biennial**

Project 17 is committed to protecting the privacy of clients, staff and volunteers. Project 17 works with clients with a range of vulnerabilities and we take the management of personal information seriously. We process a wide range of data in the course of our day to day work, including information about employees, volunteers and clients. This information enables us to deliver services and operate the organisation. To comply with the law, information is collected fairly, stored safely and not disclosed unlawfully to any other party.

This policy has been written in accordance with the General Data Protection Regulations (GDPR). This policy applies to all employees, volunteers, contractors and Trustees, as well as clients, training participants and anyone else whose data we may process in the course of Project 17's activities.

Project 17 is a Data Controller for the purposes of the GDPR. If you have any questions regarding the management of personal data, please contact the Director at the above address.

1) GDPR Principles

In accordance with the principles of the GDPR, Project 17 will ensure that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- 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 ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 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');
- 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 ('storage limitation');
- 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) Responsibilities:

We take protecting data very seriously. The Board of Trustees, together with the Director, are responsible for ensuring that the Privacy and Data Protection Policy is implemented in all service areas. Data is stored on a cloud-based server, with appropriate password security protection.

Employees, volunteers, contractors and Trustees will:

- Check that any information that they provide to Project 17 in connection with their role is up to date and accurate
- Inform Project 17 of any changes or errors
- Comply with guidelines below when collecting information about other people (e.g. clients)
- Ensure data is secure by complying with the Case Management Policy and the Confidentiality Policy, including:
    - keeping paper copies in locked filing cabinets and shredding information when it is no longer required
    - Uploading information to relevant restricted areas of the shared drives
    - Keeping computers and phones password protected and locked when not in use
    - Not storing sensitive information on removable discs
    - Keeping passwords private and secure
    - Not sharing personal data through personal email accounts or text messages
- Undertake Privacy Impact Assessments when designed or significantly changing systems or processes
- Only share information with other organisations in line with the Confidentiality and Safeguarding Policies, and in line with the GDPR
- Ensure personal information is not accidentally disclosed. Accidental disclosure of client information is a disciplinary matter

Clients are responsible for ensuring that personal data provided to the organisation is accurate and up to date.

3) Lawful basis

Under the GDPR, the lawful bases for processing data include:

- Consent of the data subject
- Necessity to comply with a legal obligation
- Necessity to protect the vital interests of a data subject or another person
- Necessity for the performance of a task carried out in the public interest in the exercise of official authority vested in the controller
- Necessity for purposes of legitimate interest pursued by the controller or a third party, except where such interests are overridden by the interests, rights and freedoms of the data subject

The conditions for processing special categories of data are:

- Explicit consent, unless reliance on consent is prohibited by EU or member state law
- Necessary for carrying out obligations under employment, social security, social protection law or a collective agreement

- Necessary to protect the vital interests of a data subject where the subject is incapable of giving consent
- Necessary for the establishment, exercise or defence of legal claims
- Necessary for assessing the working capacity of the employee
- Necessary for reasons of public interest in the area of public health

Project 17 processes data in the following ways, relying on the conditions explained below.

Client data: The main purpose of holding client data is to provide advice and advocacy services. Client data may also be used to inform our policy and research work to further our charitable objectives. Personal data will be processed by relying on the following principles:

- **Consent:** before working with a client, we will ensure that we have the client's explicit consent to store and process their data. When taking on a client the individual will be asked to sign a consent form. When taking details of an initial enquiry over the phone, verbal consent will be sought and noted on the form (see also Confidentiality Policy and Case Management Policy). Consent to act on a client's behalf or to contact a client can be withdrawn at any time and the client's case can be closed upon request. However, data will continue to be stored, relying on one of the following lawful bases.

- **Legitimate interests:** in specific situations, we may require personal data to pursue our legitimate interests as part of running the organisation. We will do this in a way that does not materially impact on individuals' rights, freedoms or interests. This might include using data to support policy and advocacy work or providing information to auditors. And/or;

- **Legal compliance:** We may need to collect and process data as required by law. For example, it may be necessary to pass on details of people posing a risk of significant harm to others. And/or;

- **Defence of legal claims:** After a client's case is closed, we will retain data for monitoring and archiving purposes. We must retain data for 6 years to protect ourselves against any legal claims that may arise following the advice we give. After 6 years information will be deleted as the limitation period will have expired. Project 17's consent form informs clients that their information will be stored confidentially for a period of 6 years following the closure of their case.

Staff, job applicant, volunteer and trustee data:

- **Legitimate interest:** Project 17 has a legitimate interest in processing data to ensure the smooth running of the organisation. And/or;

- **Defence of legal claims:** Data will be retained for 6 years following the end of the relationship with Project 17 in order to protect the organisation from legal claims that may be brought against it. And/or;

- **Working capacity of employees:** Special categories of data may also be required to assess the working capacity of employees. And/or

Others:

- **Consent:** Consent will be sought from other parties, including donors and campaign subscribers to process their data.

Processing special categories of data

It will often be necessary to process information relating to special categories of data, including (but not limited to) information relating to gender, disability, race and nationality. The legal bases on which this data can be processed are outlined above.

4) **Individuals rights:**

Individuals (including staff, volunteers, trustees, contractors, clients, training participants, S17 Hub members) have the following rights:

- **Accessing information:** Individuals have the right to access any personal data that is kept about them by the organisation. Staff, volunteers and Trustees should contact the Director to access this information. Clients should contact their adviser. Personal data will be provided by Project Seventeen upon request for access, where such request provides sufficient information for Project Seventeen to locate the personal data sought and for Project Seventeen to be satisfied as to the identity of the person making the request. Clients may also make verbal requests for access to their personal data. All requests should usually be responded to within 30 days . If the request is complex or onerous and more time is required, the individual will be notified within 30 days and an explanation will be given as to why an extension is needed.

- **Correction of personal information:** Individuals can ask for personal data that is incorrect, incomplete or out of date to be corrected. Such requests can be made in writing or verbally and will be responded to within 30 days. If the data refers to a mistake that has subsequently been resolved, then the record may be deemed as accurate. In such circumstances the fact that a mistake was made and the correct information will be included in the individual's data. Where the data in question is an opinion, as long as the data accurately records that opinion and whose opinion it is, it may not be considered as inaccurate and therefore requiring rectification. In such circumstances the individual's data shall be updated to record that the accuracy of the opinion is disputed.

- **Deletion of personal data:** Individuals can request that the information we hold about them is deleted, for example by withdrawing consent. However, Project 17 may have a legitimate overriding interest in holding the data or may be required to hold it to comply with our own legal obligations (see above). If we choose not to action a request, the reasons for this decision will be explained to the individual.

5) **When we collect data**

We normally collect data when it is provided to us by the individual. This might be through an appointment, on the telephone, through email, text message or by post. We may also collect data provided by a third party (e.g. referral partner, health visitor, or a local authority).

6) **What data we collect**

We collect data that is necessary to carry out the purpose agreed between the organisation and the individual. It is likely to include information like names and addresses, as well as sensitive

information like nationality, race, disability and gender. When working with a client we will also collect information about the case, including detailed financial information.

7) Who we share data with

We sometimes share data with third parties. For instance, we may refer a client's case to a solicitor or contact a local authority to request support on their behalf. Consent will be sought and recorded before personal information is shared. In some circumstances personal data may be shared without consent, such as when required for safeguarding purposes, to comply with the law or to prevent a crime.

8) Where data is processed

Our electronic information is stored on Google Workspace, Microsoft 365, Quickbooks and Advice Pro, all of which have confirmed their compliance with the GDPR.