St Paul's Community Development Trust

Data Protection Policy 2018

St Paul's Community Development Trust holds data about our employees, suppliers, trainees, students, volunteers and users to allow it to work with them. This policy sets out how we seek to protect personal data and ensures that staff and other members of the Trust understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Designated Data Controller be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business Purposes: The purposes for which personal data may be used by include:

- to provide services to the public in a particular geographical area as specified in our constitution,
- administer membership records,
- to fundraise and promote the interests of the Trust,
- manage our employees and volunteers,
- to manage our payroll,
- maintain our own accounts and records,
- compliance with our legal and regulatory obligations,
- compliance with our safeguarding obligations,
- Investigation of complaints,
- the checking of references as part of our recruitment process.

Personal Data: Any information relating to any identifiable individual, which will be processed and stored within an organised filing system. This can be written, in an electronic format, printed, taped, photographic, video or other formats. Personal data we may gather include:

- personal details,
- family details,
- details of lifestyle and social circumstances,
- membership details,
- goods and services,
- financial details,
- education and employment details,

Data Users: Staff, trainees, students, volunteers or others who process data.

Data Subject: The person about whom the data concerns.

Sensitive Data: Personal data relating to any of following is deemed to be sensitive personal data and must be dealt with in accordance with this policy.

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a Trade Union
- Their physical or mental health or condition
- Their genetic data
- Their biometric data
- Their sexual life
- The commission or alleged commission of any offence, or
- any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Controller: A person who determines the purposes and manner in which, personal data is, or should be processed.

Processing: Covers anything which is done with or to the data, including:

- Obtaining data recording or entering data onto the files
- Holding data, or keeping it on file without doing anything to it or with it
- Organising, altering or adapting data in any way
- Retrieving, consulting or otherwise using the data
- Disclosing data either by giving it out, by sending it on email, or simply by making it available
- Combining data with other information
- Erasing or destroying

Scope

This policy applies to the processing of all personal and sensitive personal data processed for and behalf of the Trust regardless of the format, type or methods used during processing and storage.

This policy and any accompanying procedures apply to all employees, volunteers, trustees and members of the Trust and any other person authorised to process personal data on behalf of the trust.

Failure to follow the Data Protection Policy may result in disciplinary proceedings. Unauthorised access to records or inappropriate use of Trust data that is classed as confidential or highly confidential may be treated as gross misconduct.

Data Protection Registration

St Paul's Community Development Trust – PZ 5710759

Any person, who considers that the Policy has not been followed in respect of personal data about themselves, or others, should raise the matter with the Designated Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

Who is responsible for this policy?

Responsibility for the production, maintenance and communication of this policy and procedures will be the responsibility of the Information Management Committee.

This policy and its procedures have been approved by the Chief Executive and Board of Trustees.

As our Designated Data Controller **Matthew Humpage** has overall responsibility for the day-to-day implementation of this policy.

Designated Data Controller's responsibilities:

- Keeping the Board of Trustees updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all staff and other members of the Trust.
- Answering questions on data protection from staff, trustees and other members of the Trust.
- Responding to individuals such as clients and employees who wish to know which data is being held by St Pauls Community Development Trust.
- Checking and approving with third parties that handle the Trust's data any contracts or agreement regarding data processing.

Responsibilities of the Senior Network Administrator

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Mitigation of risk and malicious damage to the Trust's network and data systems

Responsibilities of the Information Management Committee

- Approving data protection statements attached to emails and other marketing information.
- Coordinating with the Designated Data Controller to ensure all communication initiatives adhere to data protection laws and the Trust's Data Protection Policy.

- Conducting regular data audits across the Trust to ensure data is processed in accordance to the Trust's Data Protection and Information Security Policies.
- To maintain a register of the Trust's data assets including retention schedules.

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless it meets following conditions:

- We have the informed and unambiguous consent of the data subject to process their data for specific purposes. The data subject has the right to withdraw consent at any time. Consent will not be valid unless separate consents are given for different processing activities.
- Processing is necessary for the performance of a contract with the data subject or is necessary to take steps to enter into a contract.
- Processing is necessary for compliance with a legal obligation.
- To protect the vital interests of a data subject or another person.
- For public interest.
- For the legitimate interests of the Trust.

The processing of all data must be:

- necessary to deliver our services,
- in our legitimate interests and not unduly prejudice the privacy of individuals.
- In most cases this provision will apply to routine business data processing activities.

We will ensure that any use of personal data is justified using at least one of the conditions of processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for processing personal data

We will process personal data in compliance with all six data protection principles within the General Data Protection Regulation (GDPR). We will document the justification for the processing of sensitive data.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Sensitive personal data

Where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. process ethnic origin data of applicants as part of our recruitment process in order to fulfil our obligations under the Race Relations Act 2000). Any consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Designated Data Controller.

Your personal data

You must take reasonable steps to ensure that personal data we hold about individuals are accurate and updated as required. For example, if your personal circumstances change, please inform the relevant department (i.e. Payroll & Human Resources) so that records can be updated.

Information Security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Designated Data Controller will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

All staff, volunteers, trustees and other members of the Trust are required to handle and process personal data in accordance with the Trusts' **Information Security Policy, Information Handling Procedures** and other relevant procedures.

Data Retention

The Trust must retain personal data no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

St Paul's Community Development Trust

Privacy Notice – transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for the Trust. We will ensure that all data processing activities carry adequate privacy notifications. The following are details on how we collect data and what we will do with it:

What information is being collected?
Who is collecting it?
Why is it being collected?
How will it be used?
Who will it be shared with?
Identity and contact details of any data controllers?
Details of transfers to countries outside of the EEA and safeguards put in place
Retention Period

Right of Information and Access

Individuals have the right to access any personal data that is being processed by the Trust. Anyone who wishes to exercise this right should contact the Designated Data Controller in writing and provide valid proof of their identity before any information is released.

An individual has the following rights in regards to a data controller:

- To obtain confirmation of whether their data personal data are being processed
- To obtain a copy of the data being processed
- To be provided with supplemental data about the processing of their data

The trust will endeavour to do the following:

- Respond to any request made with 30 days
- Provide a free copy of the data being processed. Additional copies may be subject to a reasonable administration charge.
- To provide information in an electronic format if required.
- Supplemental information will be provided on the purposes of processing, the categories of data processed and the recipients or categories of recipients.
- The trust is also required to provide information in regards to the expected retention period of the information, or the criteria used to determine the length of retention.

- Individual must also be supplied with the source of the data (if not collected from the data subject).

Where a request is deemed to adversely affect others, the trust reserves the right to not comply with a Right of Information and Access request. The individual concerned will be notified of the reason for this decision to not comply with their request.

Portability of Data

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within 30 days, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data be transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Designated Data Controller about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Designated Data Controller will be responsible for conducting Privacy Impact Assessments and ensuring all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International Data Transfers

No data may be transferred outside of the EEA without first discussing it with the Designated Data Controller. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Report breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (ICO) of any compliance failures that are material either in their own right or are part of a pattern of failures

Please refer to out Compliance Failure Procedure for our reporting procedure.

Data Auditing and Security Planning

The Information Management Committee will conduct regular data audits to manage and mitigate risks, which will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

The Committee will produce a security plan which will take into account the results of the audit. The Committee will report the key findings of the security plan to the Trustees on an annual basis.

Training

All staff and volunteers will receive training in this policy. Data Protection training is mandatory and new staff should be enrolled on the next available course. Training should be renewed every 2 years or whenever there is a substantial change in the law or our policy or procedures.

Related Policies & Procedures: Information Security, Information Handling Procedures, Use of email and the internet procedures, Data Retention and Destruction; Disciplinary; Freedom of Information; Safeguarding.

Amended January 2018