Data Protection Policy 2020

St. Paul's Community Development Trust holds data about our employees, volunteers, trustees, members, suppliers, trainees, students, and users to allow it to work with them. This policy sets out how the Trust seeks to protect personal data and ensure that those who are authorised to collect and process personal do so lawfully.

Part One – General Data Protection

1.1 Data Protection Registration

The Trust is registered with the Information Commissioner's Office as a Public Authority as defined by the Freedom of Information Act 2000. The Trust's registration number is **PZ5710759**.

1.2 Policy scope

This policy is designed to ensure that the Trust is compliant with all current data protection legislation that is in effect from 31st January 2020 within the United Kingdom and applies to the processing of all personal and special category and criminal records 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 or organisation authorised to process personal data on behalf of the Trust. Henceforth referred to as "Staff".

Failure to follow this policy, or any action that leads to unauthorised access of records or inappropriate use of Trust Data classified as **confidential** or **highly confidential** will be treated as gross misconduct and will result in disciplinary proceedings.

Any person who considers that this Policy has not been followed in respect to processing of their own personal data, that of others should raise the matter initially with the Trust's Data Protection Officer. If the matter is not resolved it should be raised as a formal grievance.

1.3 Responsibilities for this policy

The production, maintenance and communication of this policy and its procedures will be the responsibility of the Trust's **Data Protection Officer** and the **Information Management Committee**.

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

Responsibilities of the Data Protection Officer (DPO)

Current data protection legislation requires a public authority or body to appoint a DPO. The Trust is registered as a Public Authority as defined by the Freedom of Information Act 2000 and is therefore required to appoint a DPO.

The DPO will assist in the:

- Monitoring of internal compliance, to inform and advise on the Trust's data protection obligations.
- Ensuring the Trust keeps appropriate records of its processing of personal data.
- Provide advice regarding Data Protection Impact Assessments (DPIA).
- Act as a point of contact for data subjects and the ICO.
- Ensure the Board of Trustees are updated about the Trust's data protection responsibilities, risks, threats and issues.
- Review data protection procedures and policy on a regular basis.
- Arranging data protection training and advice for all staff and other members of the Trust.
- Responding to individuals, who wish to exercise their rights and freedoms with respect to Trust's processing of their personal data.
- Checking and approving third party organisations that may act as processors where the Trust is the controller and ensuring that appropriate agreements are in place.

Responsibilities of IT Support Team

- Ensure all systems, services, software, and equipment meet acceptable security standards
- Ensure that security hardware and software is function properly
- Mitigation of risk, threats and malicious damage to the Trust's network and systems

Responsibilities of the Information Management Committee

- Approving data protection statements attached to emails and other marketing information.
- Co-ordinating with the DPO to ensure all communication initiatives adhere to data protection legislation and this Policy.
- Conducting regular data audits across the Trust to ensure data is processed in accordance with this policy and the Information Security Policy.
- To maintain a register of the Trust's data assets including the retention schedule.

2.1 Scope of processing

Personal data shall be defined as:

- Any information relating to any identifiable individual which can be processed and stored within an organised filing system.
- This can be in any format including, but not limited to:
    - written
    - electronic
    - printed
    - recorded
    - verbal
    - photographic
    - video

Personal data the Trust may gather include, but is not limited to:

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

Processing activities can be defined as, but not limited to:

- obtaining data recording or entering data on to the files
- holding data or keeping it on file without doing anything to or with it
- retrieving data, consulting or otherwise using the data
- disclosing data either by giving it out, sending it by email or simply making it available
- erasing or destroying the data.

2.2 Business Purposes

The Trust will collect and process personal data for the following purposes, but not necessarily limited to:

- to provide services to the public in a particular geographical area as specified in the Trust's constitution,
- to administer membership records,
- to manage employees and volunteers who work for the Trust,
- to manage the payroll of the Trust,
- to maintain the accounts and records of the Trust,
- to comply with legal and regulatory obligations,
- to uphold obligations regarding safeguarding of children and the vulnerable,
- for the investigation of complaints submitted to the Trust,
- for the checking of employment references during the recruitment process.

2.3 Data Protection Principles

The processing of personal data must be undertaken in accordance with the ***Principles relating to processing of personal data***, **(Article 5, General Data Protection Regulation)**. These principles state that personal data should be processed:

a) Lawfully, fairly and in a transparent manner - *("lawfulness, fairness and transparency").*
b) Collected for specific, explicit, and legitimate purposes. The data collected cannot be further used for any purpose that is incompatible with the original purpose for which it was collected - ("*purpose limitation").*
c) Adequate, relevant, and limited to what is necessary for the purposes it was collected - (*"data minimisation"*).
d) Accurate and where necessary kept up to date, with every reasonable step being taken to ensure that there are no inaccuracies – *("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 – *("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")*

2.4 Lawful basis for processing personal data

Lawful Basis for processing

A valid lawful basis is required the for processing of any personal data under Article 6 of the GDPR. There are six available:

a) **Consent:** the individual has freely given clear and informed consent for the Trust to process their personal data for a specific purpose. Removal of consent should as easy to request for the data subject as granting it.
b) **Contract:** the processing is necessary for a contract that the Trust has with the individual, or because they have been asked to take specific steps before entering a contract.
c) **Legal Obligation:** the processing is necessary for the Trust to comply with the law.
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for the Trust to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for the Trust's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

2.5 Accountability principle

Paragraph 2, Article 5 of the GDPR requires that the Trust is able to take responsibility for and demonstrate compliance with the other data protection principles. This includes:

- Ensuring that adequate records of processing activities are kept and are available to the request of the data protection officer or the ICO.
- Records must document how the processing complies with the other GDPR Article 5 principles as set out above.
- Staff who are responsible for processing the personal data are required to know and understand the conditions they rely upon for processing the data.
- The purpose and conditions for processing will be available to data subjects in the form of a privacy notice.

3.1 Special Category data (Sensitive Information)

The Data Protection Act 2018 and GDPR require that special categories of data that are particularly sensitive to the data subject require an additional processing condition. This is because the unlawful exposure of such data could have a significant impact on the rights and freedoms of data subjects concerned since unlawful processing or sharing of the data concerned has the potential be used in such a way that it could lead to unlawful discrimination.

Special category data includes the following information:

- Race and ethnic origin,
- Religious or philosophical beliefs,
- Political opinions,
- Trade union membership,
- Biometric data used to identify and individual,
- Genetic data,
- Health data,
- Data related to sexual preferences, sex life and/or sexual orientation,

3.2 Additional conditions for processing (Article 9 GDPR)

The Trust must be able to demonstrate a lawful reason for collecting and processing special category data of any nature. Therefore, it is prohibited to collect and process these data unless it meets one of the following conditions:

a. Explicit consent is sought and granted by the data subject.
b. Employment, social security, and social protection (if authorised by law).
c. To protect the vital interests of the data subject or another identifiable individual.
d. Processing is carried out by a not-for-profit body or foundation with a political, philosophical, religious or trade union aim.
e. Data is made public by the data subject.
f. Legal or judicial acts.
g. Reasons of substantial public interests (with a basis in law).

h. Health and social care (with a basis in law).
i. Public health (with a basis in law).
j. Archiving, research, and statistics (with a basis in law).

3.3 Processing of special category personal data

1. In the first instance it is the policy of the Trust to always seek the valid and explicit consent of the data subject for the processing of any special category data where appropriate.

2. The Trust must also keep adequate records to demonstrate that explicit consent was freely given and remains valid.

3. The Data Protection Act 2018 sets out the lawful grounds for the processing of special category data ***without*** consent if the circumstances justify it if in the ***substantial public interest*** in order to safeguard children or individuals at risk. ***(Schedule 8, Section 35(5) Data Protection Act 2018)***

4. Lawful basis ***(b), (h), (i) or (j)*** also require that the processing meets the associated condition in UK law, set out in ***Part One, Schedule One of the Data Protection Act 2018***

5. If the processing relies on "**substantial public interest"** ***(Article 9(2)(g), GDPR)*** it must also meet one of 23 specific public interest conditions set out in ***Part Two of Schedule One of the Data Protection Act 2018***.

6. The Data Protection Officer will be responsible for ensuring that the processing of any special category data is justified under an appropriate lawful basis and that the appropriate additional ***Schedule One*** processing conditions are applied in the form of an "**Appropriate Policy Document"** where necessary**.**

7. Special category processing will also be subject to regular review through internal audit to ensure that processing continues to be justified and lawful.

4.1 Processing of Criminal Records

Any criminal records checks are justified by law under the Rehabilitation of Offenders Act 1974. Criminal records checks cannot be undertaken based solely on the consent of the data subject.

5.1 Use of CCTV

CCTV footage of individuals is personal data and therefore subject to data protection regulations. Individuals have the same rights of access as any other form personal data.

The Trust will be the data controller where footage is recorded on it premises and environs. The Trust will have a separate CCTV policy that conforms to the ICO's CCTV Code of Practice, but for the purposes of data protection the following is stated as policy:

1. The principal purposes of the Trust's CCTV systems are as follows:

   a. For the prevention, reduction and detection of crime and other incidents.
   b. To ensure the safety of staff, students, and visitors.
   c. It may also be used to monitor staff when carrying out work duties.
2. Information processed may include visual images, sound recordings, personal appearance, and behaviours.
3. The Trust seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy
4. Signage will be in place notifying individuals that recording is taking place and access to the system will be restricted to authorised members of staff.

Part Two – Rights of the Data Subject

6.1 Your personal data

Members of staff must take reasonable steps to ensure that the data held by the Trust are accurate and updated as required. For example, a change in personal circumstances should prompt a member of staff to notify the relevant department (i.e. Payroll or Human Resources) so that records can be updated.

7.1 Subject Access Requests.

Data protection legislation gives a data subject the right to access the information that the Trust processes about them. Accessing data in this way is known as a 'making a Subject Access Request'

An individual is entitled to the following:

- To obtain confirmation of whether the Trust is processing their personal data.
- To obtain a copy of the data that is being processed, subject to any applicable exemptions and the removal of other people's personal data as appropriate.
- To be provided with supplemental data about the processing of their data.

The Trust will endeavour to undertake the following:

1. Respond to any request made within one month from the data the request was submitted.
2. Respond to requests for educational records within 15 school days.
3. Provide a free copy of the data being processed. Additional copies may be subject to a reasonable administration charge.
4. Provide data subjects with supplemental information on the purposes for processing, the categories and expected retention periods for the personal data.

7.2 Submitting a Subject Access request

A subject access request to the Trust maybe submitted in whatever form the data subject wishes, however the Trust has created a standard Subject Access Request Form which may be completed ad emailed to dpo@stpaulstrust.org.uk, or posted to the address on the form. Using the form will enable the Trust to verify the individual's identity and ensure a timely and accurate response. Reasonable steps should be taken to ensure that any Subject Access Requests made by another person other than the data subject on behalf of the data subject have the appropriate authority to make the request.

1. Staff who receive a subject access request should inform the data protection officer immediately upon receipt.
2. On receipt the data protection officer will contact the individual making the request acknowledging its receipt and confirming the statutory deadline by which they will receive a reply. **For the avoidance of doubt this is one calendar month from the date the request was made.**
3. If the individual is not satisfied that Trust has dealt correctly with the request, they should contact the data protection officer at dpo@stpaulstrust.org.uk. If they are still not satisfied with the response, then they should contact the ICO.

7.3 Subject Access Requests by children or on their behalf

Where the Trust receives a request for information about children, the following must be taken into consideration when responding:

- Even if a child is too young to understand the implications of a subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian.
- It is the child who has the right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.
- Consideration of whether the child is mature enough to understand their rights when responding to a request. If you are confident that the child can understand their rights, then the response should be made directly to the child.
- However, the parent may be allowed to exercise the child's rights on their behalf if the child authorises it, or it is evident that this is in the best interests of the child.
- When considering borderline cases, the following should be considered along with other relevant information that may impact on each individual case:
    - The child's level of maturity and their ability to make decisions,
    - The nature of the personal data
    - Any court orders relating to parental access or responsibility that may apply,
    - Any duty of confidence owed to the child or young person,

- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- Detriment to the child or young person if individuals with parental responsibility cannot access this information.
- Any views the child or young person has on whether their parent(s) should have access to information about them.

7.4 Exercising other data rights

Data protection legislation gives a data subject other rights in relation to their personal data. An individual can submit a rights request in whatever form the wish, but the recommended method is to email the data protection officer at dpo@stpaulstrust.org.uk to ensure a timely response.

An individual submitting a rights request will need to be as specific as possible about what personal data they are asking to be either:

1. Rectified,
2. Erased,
3. Restricted,
4. Ported,
5. State the nature of their objection to the purpose of its processing.

As with Subject Access Requests a form of photographical ID will enable the Trust to swiftly verify the individual's identity and right make the request about the data concerned.

Part Three – Security, Retention and Data Sharing

8.1 Information Security

Anyone authorised to process personal data on behalf of the Trust (including authorised third-party processors) must ensure that data is secured against loss, misuse, or unauthorised access.

Anyone authorised to process personal data on behalf of the Trust must do so in accordance with the Trust's Information Security Policy and procedures, in particular (but not limited to):

- Information Handling Procedures
- Use of Email and internet Procedures
- Mobile and Remote Working Procedures

8.2 Data Retention

The Trust must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into consideration the reasons why the personal was obtained. This should be determined in a manner consistent with the Data Archiving, Retention and Destruction Policy and the Data Retention Schedule.

9.1 Data Sharing

Current data protection legislation sets certain restrictions and conditions as to when the Trust is able or required to share personal data with third-party organisations. This is to ensure that the personal data are adequately protected and handled by other appropriately.

The Trust is required to share personal data with other organisations as required to provide its services and fulfil its legal obligations or require a third party to process certain data on its behalf.

Data sharing will be classified into three broad categories:

i. **Category One:** The sharing of personal data with a third party used for **Joint Purposes**
ii. **Category Two:** The passing of personal data to a third party for its **Own Purposes.**
iii. **Category Three:** Engaging a third party to handle, share or otherwise use certain personal data on behalf of the Trust.

On occasions, the sharing of personal data is obligatory under law (usually Category Two), but usually it is at the Trust's discretion whether or not to share personal data.

The following restrictions and conditions differ depending on the type of sharing in question:

1. The Trust will not store personal data outside the United Kingdom or European Economic Area without the explicit consent of the data subject
2. All reasonable efforts will be made to ensure Trust data that is currently stored within the EEA is repatriated to the United Kingdom before December 31st, 2020. Where this does not prove possible, the Trust will ensure that Data sharing agreements are in place the contain standard clauses to ensure the necessary are in place for the sharing of data to take place on the basis that the UK is a Third country.
3. The individuals whose personal data is involved have been informed about the sharing, whether in the Trusts Data Security and Privacy Statement, or in supplementary notices supplied for specific purposes and categories of data subject
4. Consideration has been given as to how to share the minimum amount of personal data necessary to achieve the required purposes.
5. Consideration has been given as to the length of the sharing agreement and will happen at the end of it.
6. Consideration has been given as to how to share personal data securely in compliance with the Trust's Information Security Policy and procedures. (e.g. use of encrypted email and storage devices to ensure safe transmission)
7. The sharing is documented and can be audited.

9.2 Sharing personal data with a third party for joint purposes (Category One sharing)

Where the Trust share data with a third party for joint purposes, the organisations are known as "Joint Controllers" (Article 26 GDPR). The sharing is usually long terms or ongoing. In these circumstances, it is mandatory to:

- Have a documented arrangement (not necessarily a contract) setting out the respective roles and responsibilities with regard to data protection matters, including who individuals can contact if they want to complain or exercise any of their rights and freedoms under current data protection legislation.
- Be transparent, by making the essence of this arrangement available to the individuals whose data is shared, if not already included in a privacy notice.

9.3 Sharing personal data with a third party for its own purposes (Category Two sharing)

Where the Trust shares personal data with a third party for its own purposes, each organisation is a separate "Data Controller". The sharing might be "one-off," long term or ongoing. The third party might be closely 'related' to the Trust such as another local group or organisation or wholly unrelated to the Trust (such as HMRC).

In these circumstances, there are no mandatory restrictions or conditions, but it is advisable to do the following unless the sharing is required by law:

- Conduct and document due diligence checks to ensure that the arrangement has been carefully considered in line with the general points above.

9.4 Using a data processor: Sharing personal data with a third party for its own use on behalf of the Trust (Category Three sharing)

Where the Trust shares personal data, it controls with a third party to carry out operations in relation to that data on behalf of the Trust, the third party is known as the 'data processor'. (Article 28, GDPR).

The sharing might be one-off, long term or ongoing and it applies primarily to situations where the Trust is outsourcing or offering a function that involves the processing of personal data (whether storage or more active management that ordinarily it could do by its own merit).

In these circumstances the Trust must obtain a binding contract that committing the data processor to standards in relation to:

- Security
- The engagement of 'sub-processors'
- Assisting the Trust to meet data protection obligations with regard to individual's rights and freedoms.
- Co-operating with Trust audit and inspections if applicable.

Part Four – Data Protection by Design, Techniques and Practices

10.1 Data Protection and privacy by design

The Trust is required to embed concepts of data protection and privacy "by design" at the earliest stage of any new or proposed processing activity, project or procedure. This has a bearing on initiating an IT based project, such as a new system or database which will involve processing personal data, especially special category data. In this regard, adopting a data protection by design approach can trigger the need for a full Data Protection Impact Assessment to assess and document the risks to data subjects and the mitigating measures that might need to be adopted to be implemented.

10.2 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is legally required where any proposed data processing is likely to result in a high risk to the interests, rights and freedoms of data subjects. This is applicable particularly in circumstances that involve:

- large scale (automated) profiling,
- processing of special category personal data
- the monitoring of public areas.

A DPIA takes the form of a document completed following consultation with relevant stakeholders, including the data protection officer and a sample of the data subjects themselves.

The following areas should be given due consideration in order to assess the necessity for a full and formal DPIA to be carried out:

- Describe the nature, scope, context, and purposes of the proposed data processing
- Assess the necessity of the proposed processing
- Identify ad assess the risks to individuals
- Identify ay additional measures to mitigate those risks

If a completed DPIA reveals that the risks to data subjects cannot be adequately mitigated, ICO must be consulted for a formal opinion.

11.1 Data pseudonymisation

Data pseudonymisation is a technique that replaces or removes information in a data set that identifies individuals. This allows data sets to be shared in such a way that the personal data cannot be attributed to a specific individual without the use if additional information. However, the additional information needs to be kept ***separate*** and ***secure*** from the main data set. All information relating to that data set are subject to the same Information Security data classification. (i.e. confidential or highly confidential depending on the nature of the data set).

It is important to remember that pseudonymised data sets which could be attributed to an identifiable individual by use of the key or additional information should still be

considered to be ***"information on an identifiable natural person"*** (GDPR, Recital 26). In this respect this policy will apply in full to data that has been pseudonymised regardless of its purpose and be subject to current data protection legislation.

11.2 Data anonymisation

Data protection legislation does not apply to personal data that has been anonymised. (GDPR Recital 26). Anonymisation can therefore be a method of limiting the Trust' risk and a benefit to data subjects when sharing certain data sets. For data to be considered truly anonymised it will be necessary to remove all **direct** and **indirect** personal identifiers within the data set. Only then will the data set not be subject to this policy or data protection legislation.

12.1 Processing personal data of children

Data protection law states the ***"children's personal data merits specific protection as they may be less aware of the risks, consequences and safeguard concerned and their rights in relation to the processing of their personal data (Recital 38, GDPR)***

It is important that staff are aware of the need to give due consideration when undertaking activities that may involve collecting data from children with no interaction from their parents or those with parental responsibility.

Staff should always consult the Trust's Safeguarding Policy and Use of Internet and Email Procedures in the first instance when planning any such activity; especially where an online service may require consent of the user.

Due consideration should be given to the lawful basis of any processing activity prior to its undertaking. Should any doubt remain the data protection officer should be consulted and DPIA carried out if necessary, to assess any unmitigated risks. Staff such be mindful that under UK law only children over the age of 13 are able to provide consent to the processing of their own data without recourse to those who hold parental responsibility.

If preventative or counselling services are offered or a child is referred to such a service, then parental consent should not be a condition for any data processing to allow a child to access to the service.

13.1 Privacy and Electronic Communications Regulations

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) sit alongside data protection legislation. All processing of personal data is governed by data protection legislation, but when this processing involves electronic communications, some additional rules apply in the form of the PECR.

The Trust must consider the following aspects of PECR when conducting any of the following activities in order to protect the individual's specific privacy rights and apply to:

- Marketing by electronic means, including marketing calls, texts, emails and faxes
- The use of cookies or similar technologies that track information about individuals who access a website or other electronic service.

These rules apply in relation to the use of email distribution lists and web services that ay be used for direct marketing purposes to individuals. The Trust should ensure that there are appropriate consents in place before undertaking any marketing activity that may be subject to PECR and where doubt remains consult the data protection officer for clarification.

14.1 Reporting Data Breaches

All members of the Trust have an obligation to report actual or potential breaches or failures of Information Security that may be expose personal data to unauthorised or unlawful access using the Data Breach Reporting Procedure. However, the data protection officer should be consulted relating to a breach or failure of Information Security in the first instance.

Carrying out the Data Breach reporting procedure will enable the Trust to:

- Investigate the breach or failure and take remedial steps if necessary
- Maintain a register of compliance failures and learn relevant lessons that enable the Trust to prevent a recurrence in the future
- Make an initial report to the ICO and any affected, processors, joint controllers or controllers within 72 hours of becoming aware of any material breach that may impact the rights and freedoms of the affected data subjects.

15.1 Data Auditing and Security Planning

The Information management Committee will conduct regular data audits to manage and mitigate risk which will inform the Trust's data register. This contains information on what data is held, where it is stored, how it is stored and used and who is responsible for the data. Furthermore, it includes information of any addition regulations and retention timescales that may be relevant.

The Committee will produce a security plan which will consider the results of the audit. The Committee will report the key findings from the implementation of the security plan to Trustees on a annual basis.

16.1 Staff Training

All staff, volunteers, trustees, and school governors 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 on an annual basis or whenever there is substantial change in the law or the Trust's policies and procedures.

Related Policies and Procedures

Information Security Policy, Information Handling Procedures, Use of Email and the Internet procedures, Data Archiving, Retention and Destruction Policy, Data Retention Schedule, Disciplinary Policy, Freedom of Information Policy & Safeguarding Policy.

Amended November 2020