

	<h2>Data Protection Policy</h2>
<p>Company no: 563463 Charity no: SC047335</p>	<p>Created: July 2018 Revise by: July 2019</p>

Accurate information about our community and the people who live there is vital to the work of Dollar Community Development Trust and we recognise the importance of safeguarding all this information and paying particular regard to that information which relates to individuals whether members, volunteers or staff in whatever form that information is held.

The Trust needs to keep and process certain information about individuals so that it can provide a membership service and find out about and respond to the community's ideas and needs. We also have to seek and keep some information on the people we recruit, whether staff or volunteers, and provide information from time to time to comply with the demands of statutory or funding bodies.

In doing so, the Trust must comply with the Data Protection Act 1998 and 2003, and the General Data Protection Regulation (GDPR) 2018 and process information in accordance with data protection principles.

1. Policy Objectives

- Ensure the Trust complies with data protection law and follows good practice;
- Protects the rights of staff, members, volunteers and users of the Trust's services;
- Is open about how the Trust stores and processes individual's data;
- Protects the Trust from risks of data breaches

2. Information we collect and use includes:

- Information about members – name, contact details and any information the member wishes to impart about their interest in the Trust's activities and how they might get involved. We collect this information as part of our legitimate interest.
- Information about volunteers – the same as for members and any information which might affect their health and well being in the role for which they have volunteered – also collected as part of our legitimate interest.

- Information about staff – qualifications and experience, emergency contact details, bank details, date of birth, National Insurance numbers, references, staff supervision and development records. This is required by statute and part of our legitimate interest.
- Information about personal contact with us e.g. meetings, phone calls, emails / letters
- Information classified as ‘sensitive’ personal information will only be collected and used where it’s needed to safeguard the health and well being of an individual who is working with the Trust or receiving a service from us or to comply with our legal obligations
- Information on children at risk or vulnerable adults. In these cases, we will collect and use only the information required to identify the child/adult (such as their name, age, gender)

3. Where we collect information

We may collect personal information directly from a variety of sources, including:

- A membership application
- A volunteer registration form or other volunteer recruitment processes
- Staff application forms and recruitment processes
- As required for registration with the Protection of Vulnerable Groups scheme
- Phone conversations
- Emails or letters
- Registering for one of our events e.g. our AGM or a consultation event
- Participating in research surveys to help us understand our community better and improve services

4. What we collect and use personal information for

We take privacy seriously and we will only ever collect and use information which is personal where it is necessary, fair and lawful to do so. We will collect and use personal information only where:

- People have applied for membership
- People have given us consent to send them information about our services and/or about selected third parties which we believe may be of interest and benefit to them
- People have given consent for us to use their information for research or consultancy to help us improve our services
- It’s necessary for us to meet our legal or regulatory obligations (e.g. for taxation or safeguarding purposes)
- It’s in the legitimate interests of a third party

These third parties include:

- Regulators and Supervisory Authority e.g. OSCR, the Information Commissioner’s Office for the UK (the ICO)
- Law enforcement
- Social Services
- HMRC

If a person does not wish us to collect and use personal information in these ways, it may mean that we will be unable to provide them with our services.

We will never sell personal details to someone else. Whenever we share personal information, we will do so in line with our obligations to keep personal information safe and secure.

5. Where personal information is processed

The majority of the personal information we hold is processed in the UK and European Economic Area (EEA).

In the unlikely event that some personal information may be processed by us or the third parties we work with outside of the EEA, including countries such as the United States, we will take additional steps to ensure that personal information is protected to at least an equivalent level as would be applied by UK / EEA data privacy laws e.g. we will put in place legal agreements with our third party contacts and do regular checks to ensure they meet these obligations.

6. Responsibilities

Everyone who works for or with the Trust, staff and volunteers, is responsible for ensuring data is collected, stored and handled appropriately in line with this policy and data protection principles.

The trustees have ultimate responsibility for ensuring that the Trust meets its legal obligations.

The company secretary is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection policies and procedures, within an agreed timescale;
- Arranging data protection training and advice when required;
- Handling data protection questions from staff, volunteers and anyone else covered by this policy;
- Dealing with requests from individuals to see the data the Trust holds about them;

7. How we protect personal information

We take information and system security very seriously and we will always strive to comply with our obligations. Any personal information which is collected, recorded or used in any way, whether on paper, online or any other media, will have appropriate safeguards applied in line with our data protection obligations.

Personal information is protected by controls designed to minimise loss or damage through accident, negligence or deliberate actions. Our employees and volunteers also protect sensitive or confidential information when storing or transmitting information electronically.

8. How long we keep personal information

We will keep personal information only where it is necessary to maintain someone's membership, provide someone with services or maintain their employment as staff or volunteer.

We may also keep personal information after this period but only where required to meet our legal or regulatory obligations. The length of time we keep personal information for these purposes will vary depending on the obligations we need to meet.

9. Rights within the GDPR:

- **Right to Access.** People have the right to obtain confirmation from the Trust about whether their personal data is being processed, where, and for what purpose. They also have the right to receive a copy of this.
- **Right to Be Forgotten (or Data Erasure).** People can demand that the Trust erase their personal data and stop further sharing of the data.
- **Data Portability.** People can receive their personal data in a machine-readable format and have the right to transmit that data to another organisation.

Sections 10 – 12 below set out how the Trust will ensure these rights are adhered to.

10. Right to access

The Trust respects the right of its staff, volunteers, and members to access any personal data about them which is being held by the Trust to check that it has been fairly obtained, that it is accurate, and to have such data corrected where necessary. We also recognise a person's right to withdraw consent to the processing of personal data where such processing could cause them significant damage or distress.

11. Right to be forgotten (erasure)

The Trust does not retain personal data for longer than required and will comply with any request for erasure unless this breaches statutory requirements.

Once a member of staff or volunteer has left our organisation, or a piece of work is completed, it will not be necessary to retain all the information held. Sufficient data to allow the supply of references will be kept for up to one year and data required by statutory authorities for taxation and other purposes will be kept as required by those authorities.

Information for monitoring and evaluation will, as far as possible be anonymised.

12. Data portability

The Trust maintains most of its data in machine readable format with only minimal information kept on paper, usually for a short period (e.g. membership forms are scanned to an encrypted disc as soon as practicable after receipt). This will make data portability straightforward in most instances.

It is the responsibility of all staff and volunteers to ensure that any data, whether held electronically or manually, is kept securely and not disclosed unlawfully, in accordance with the Data Protection Policy and with the General Data Protection Regulation

13. Complaints and breaches

We will always strive to collect, use and safeguard personal information in line with data protection laws. If someone believes we have not handled personal information as set out in our Privacy Policy, we will encourage them to contact us and we will do our utmost to put things right.

Where any volunteer or staff member believes a breach of data protection has occurred, the company secretary must be informed as soon as possible. All breaches, however minor they appear, will be recorded by the company secretary on a register which will be open for inspection. Where he/she believes the breach is significant he/she will inform the Information Commissioner as soon as possible.