DATA PROTECTION POLICY	POL-006: Rev. 1

KEY DETAILS	
Policy prepared by	**L Manderson, Office Manager**
Approved by Board on	**2 November 2020**
Policy became operational on	**2 November 2020**
Next review date	**2 November 2020**

RELATED DOCUMENTS	
Information Technology Security Policy	POL-003
Retention and Destruction of Documents Policy	POL-008
HR Employee Records Policy	POL-009
Privacy Notices: Board Members, Employees, Tenants, Members, Volunteers, Website	
Data Subject Access Request Form	

CONTENT

1. INTRODUCTION

Comrie Development Trust retains and processes personal information about individuals. These include members, associate members, volunteers, employees, sub-contractors, tenants, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, processed, and stored to comply with the law and to meet CDT's data protection standards.

2. POLICY PURPOSE

2.1 The purpose of this Policy is to enable CDT to comply with the Data Protection Act 2018, which incorporates the EU General Data Protection Regulations, to ensure CDT takes adequate measures to protect such personal data which has been collected, processed and stored at CDT premises.

2.2 CDT aims to:

- 2.2.1 Comply with data protection law and follow good practice.
- 2.2.2 Protect the right of its employees, its members, volunteers, tenants and partners.
- 2.2.3 Be open about how it stores and processes individuals' data
- 2.2.4 Provide training and support for its employees and volunteers who handle data such that they can act confidently and consistently.
- 2.2.5 Protect itself from the risk of a data breach

3. POLICY SCOPE

This policy applies to:

3.1 All directors/trustees of CDT Board;
All employees of CDT
All volunteers of CDT
All contractors, suppliers and any other people working on behalf of CDT.
In this policy the above are referred to as Users.

3.2 It applies to all data that CDT holds relating to identifiable, living, individuals, including personal data, sensitive personal data and any other data even if it technically falls outside of the General Data Protection Regulation.

4. POLICY REVIEW

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR.

5. DEFINITIONS

NB: For the purposes of this Policy the words "Personal Data" are used to describe Data, Personal Data and Sensitive Personal Data as defined below.

General Data Protection Regulation (GDPR)

The EU General Data Protection Regulations (GDPR) was incorporated into UK Law on 25 May 2018 under the Data Protection Act 2018. Following the UK's exit from the EU, GDPR will continue to be enforced and govern the way that personal information/data is collected, stored and processed by companies and organisations.

Data:
Data is broadly referred to as:
a) Electronic data (including CCTV recording)
b) Data forming part of a 'relevant filing system' (see definition below)

Personal Data:
Personal data means data which relate to a living individual who can be identified
a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, CDT, and includes any expression of opinion about the individual and any indication of the intention of CDT or any other person in respect of the individual.

Sensitive Personal Data:
This is data that contains information such as biometric data, ethnic origin, political opinion, religious or other belief, member of trade union, disabilities, mental health condition, sexual life, criminal record, next of kin details, salaries, employee reviews, etc.

For the purpose of CDT, sensitive personal data is all information about a living individual other than their name, address, email addresses, and phone numbers.

Relevant Filing System:
Personal data held in a relevant filing system falls under "personal data" as defined by the Data Protection Act 2018. A file is considered to be held within a relevant filing system where a file easily identifies an individual's personal data.

The Controller
The Controller determines the purposes and means of processing personal data. The Board Members of CDT act as The Controller.

Data Processor: A third party that processes information on behalf of the Controller. Processors can only be appointed under a legally binding agreement.

Lawful Basis
CDT must have a valid lawful basis in order to process personal data.
There are six lawful bases and that lawful basis must be established before processing personal data begins.

The lawful bases are:

- **Consent:** The individual has given clear consent to process their personal data for a specific purpose.
- **Contract**: processing is necessary for a contract with an individual or because they have asked CDT to take specific steps before entering into a contract.
- **Legal Obligation:** processing is necessary for CDT to comply with the law (not including contractual obligations).
- **Vital Interests:** processing is necessary to protect someone's life.
- **Public Task:** processing is necessary for an organisation to perform a task in the public interest or for the organisations official function and the task or function has a clear basis in law.

- **Legitimate Interest:** processing is necessary for CDT'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 over-rides those legitimate interests.

Subject Access Requests: Individuals have the right to know what personal data is being held about them and verify the lawfulness of the processing. They may make a written request for this information and this is known as a Subject Access Request.

6. DATA PROTECTION LAW

The Data Protection Act 2018 came into force on 25th May 2018 when the EU GDPR were incorporated into UK Law. The Act describes how organisations, including CDT, collects, processes and stores personal information.

6.1 To comply with the law, CDT must

- Only collect personal data that CDT needs for a specific purpose
- Keep it secure
- Ensure it is relevant and up to date
- Only hold as much as is needed, and only for as long as it is needed
- Allow the subject of the information to see it on request.

6.2 CDT will adhere to the principles of data protection as detailed in The Data Protection Act 2018. The principles are that personal data:

- is processed fairly and lawfully
- is obtained only for specific, lawful purposes
- is adequate, relevant and not excessive
- is accurate and kept up to date
- is not held for any longer than necessary
- is processed in accordance with the rights of data subjects
- is protected in appropriate ways
- is not transferred outside the European Union

7. RESPONSIBILITIES

7.1 Everyone who works for, or with, CDT has some responsibility for ensuring personal data is collected, stored, and processed appropriately and in accordance with this policy and data protection principles.

7.2 In order to protect CDT from the consequences of a breach of its responsibilities, users are required to read and understand their responsibilities as outlined within the Policy. If users are uncertain of their responsibilities in relation to data protection, they are required to seek guidance from the Office Manager.

7.3 The Board of Trustees each recognises their overall responsibility for ensuring that CDT complies with its legal obligations in relation to data protection.

8. SAFE MANAGEMENT OF PERSONAL DATA

8.1 Personal data collection, storage and processing should be carried out by fully observing the principles in Section 6.1 and 6.2 of this Policy.

8.2 Personal data should only be collected from information provided directly by individuals and for the purpose of aiding CDT in carrying out CDT's business.

8.3 Personal data that is no longer relevant should be deleted or destroyed.

8.4 Personal data that is held by CDT should be up to date and CDT employees should, on a regular basis, take steps to ensure that out of date data is updated.

8.5 Personal data should not be shared informally. When access to confidential information is required this should be requested, in the first instance, from the Office Manager. The Office Manager will advise on whether the information can be accessed and, when required, will obtain approval from the Board.

8.6 Personal data should only be transferred to a third party when necessary to comply with legal obligations, administering employee salaries and pensions, processing financial transactions, complying with contractual obligations, and the recovery of debt.

8.7 With the exception of 8.6, all other personal data should not be transferred to a third party without the written permission of the data subject.

8.8 Personal data should not be shared with other organisations for marketing, market research or commercial purposes.

9. SECURITY AND DATA STORAGE

9.1 CDT procedures are in place for collecting, handling, processing and storing personal data about employees, Board members, members, volunteers, and all those having a commercial relationship with CDT. These procedures will be covered in induction and training CDT Employees and Volunteers.

9.2 All personal data will be stored securely and confidentially. The only people able to access personal data should be those who require it to carry out their work.

9.3 Personal Data may be held on third party approved software when it is an essential part of processing personal data. For example, approved bookkeeping software, or when sending bulk e-mails to the membership.

9.4 Data stored in paper form will be held in locked filing cabinets or cupboards and access restricted to authorised employees and volunteers.

9.5 The Office Manager should retain an up to date list of all types of personal data collected, how and where it is stored and who has access to this.

9.6 Employees must report all incidences where any form of personal data and/or devices containing personal data have been lost, misplaced or stolen to the CDT Office Manager such that any appropriate remedial action or reporting process can be followed.

9.7 Breaches of this policy will be dealt with under CDT's disciplinary procedure.

10. SUBJECT ACCESS REQUESTS

10.1 All individuals who are the subject of personal data held by CDT are entitled to:

- Ask what information CDT holds about them and why
- Ask how to gain access to this
- Be informed how to keep it up to date
- Be informed how CDT is meeting its data protection obligations.

10.2 The individual should make their request by email or letter. All requests should be passed to the Office Manager who will establish the subject's identity prior to releasing the data.

10.3 CDT will provide the information free of charge. However, CDT reserve the right to charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee will be no more than the cost of CDT employees' time in producing the personal data or £10 per subject access request, whichever is the lower. This will be at the discretion of the CDT Board.

10.4 The Office Manager will provide this data within the timescale required under The Data Protection Act which is 40 days.

10.5 In certain circumstances, CDT may have a legal obligation to disclose personal data. In such cases CDT will ensure that it only discloses information that has been specifically requested. Where it is permitted and practicable, CDT will endeavour to inform individuals as to what information is being requested, by whom and why.

11. DOCUMENT RETENTION

11.1 Personal data will be stored only for as long as it is needed or required and will be disposed of appropriately.

11.2 Personal data held as part of CDT's historical archive will be subject to POL-008 Retention and Destruction of Documents Policy.

12. POLICY REVISION HISTORY

REVISION CONTROL			
Revision	**Author**	**Date**	**Changes**
Rev.0	L Manderson	18.6.2018	Approved by Board.
Rev. 1	L Manderson	2.11.2020	Approved by Board at Board meeting. Board authorised policies where changes were minor or where there were no changes. No changes made.