

Data Protection Policy

The Charltons Memorial Community Trust CIO

Adopted by Trustees 25/4/2023

- 1. Policy and Procedures**
- 2. The Data Protection Act**
- 3. Responsibility of the management committee of the CIO**
- 4. Procedures for handling Data and Data Security**
- 5. Privacy Notice and Consent Policy of the CIO**
- 6. Operational Guide for all trustees and volunteers of the CIO**
- 7. Definitions of terms used**

1. Data Protection Policy and Procedures

Introduction

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work of managing The Charltons Memorial Trust (CIO). This personal information must be collected and handled securely.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs. The charity will remain the data controller for the information held. The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the CIO commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

2. The Data Protection Act

This contains 8 principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s),
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by all trustees who together take appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area.

Applying the Data Protection Act within the charity

We will let people know why we are collecting their data, which is for the lawful purpose of managing the community Hall and Field, its hirings and finances. It is our responsibility to ensure the data is only used for this purpose. Unless specific consent is given or the Personal Data is already in the public domain. Access to personal information will be limited to trustees, staff and volunteers.

Where individuals need to be identified in public documents like minutes and harm may result initials rather than full names will normally be used

Correcting data

Individuals have a right to make a Subject Access Request (SAR) to find out whether the charity holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them. Any SAR must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g. passport and confirmation of address e.g. recent utility bill, bank or credit card statement.

Responsibilities

The CIO is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for.

The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- Collection and use information fairly.
- Specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
- Ensure the quality of information used.

- Ensure the rights of people about whom information is held, can be exercised under the Act. These include:

The right to be informed that processing is undertaken.

The right of access to one's personal information.

The right to prevent processing in certain circumstances, and the right to correct, rectify, block or erase information regarded as wrong information.

- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information.

All trustees, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

3 The Management Committee of the CIO has responsibility for.

- a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- b) Anybody wanting to make enquiries about handling personal information knows what to do
- c) Dealing promptly and courteously with any enquiries about handling personal information
- d) will regularly review and audit how it holds, manages, and uses personal information
- e) regular training will be provided for anyone processing personal information

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 Data Protection Act 1998.

4. Procedures for Handling Data & Data Security

The CIO has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data
- unauthorised disclosure of personal data
- accidental loss of personal data

All trustees, staff and volunteers must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone. The data controllers such as secretary treasurer and web content manager will hold information on devices that are password and malware secured.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress.

5. Privacy Notice and Consent Policy of the CIO

The private notice and consent policy are as follows: **Required on website and hire agreement and applications requesting or prudent to use as out policy.**

The CIO uses personal data for the purpose of recording information for the purpose of managing the hall, it's bookings and finances. Information on its trustees, hirers, and users. Reclaiming gift aid, and use in marketing events such as ticket information, entrants and volunteers for fundraising activities, circulation of newsletters, staff employment.

Data is only used for legitimate purpose for which it was collected securely kept and disposed of securely when no longer needed. Account information can be retained for 6 years and longer for hall insurance requirements. Minutes and communication held for 3 years then access restricted. If you would like to find out more above how we use your personal data or want to see a copy of information about you that we hold please contact the halls secretary for a subject access request (SAR).

Consent forms if used will be kept by the Secretary in a securely held electronic or paper file.

6. Operational Guidance

All trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

Emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Where someone who is not a trustee needs to be copied into an email eg wider circulation list for an upcoming event, we encourage use of bcc not cc so as to avoid PD sharing through forwarding.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous.
- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password). Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

If you do have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the

server or laptop. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Passwords:

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password:

- Common sense rules for passwords are: do not give out your password
- do not write your password somewhere on your laptop
- do not keep it written on something stored in the laptop case

Data Storage

Personal data will be stored on the preferred system of Drop box password protected to serving trustees working party volunteers or staff. Care should be taken to delete the info and communications when no longer required or trustees retired. All documents should be working documents and if not should be archived, except finance, insurance and legal documents which can be kept as long as statute requires. All documents not being actively used needing to be kept for longer than 3 years will be copied off all PC's and devices and drop box and stored on password protected USB format, labels attached and passed to the secretary or chair to keep secured in a locked file.

All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

Information Regarding Employees or Former Employees

Information regarding an employee or a former employee, the trustees will keep indefinitely for referral checking disclosure, employment law, taxation, pensions, or insurance to comply with their obligations.

Accident Book

This will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

Data Subject Access Requests

We may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the charity. The circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent are:

- a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person (eg child protection)
- b) The Data Subject has already made the information public
- c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- d) Monitoring for equal opportunities purposes – i.e. race, disability or religion

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. We intend to ensure that personal information is treated lawfully and correctly.

Photos for publicity

The ICO states we can use photos of crowds/groups for publicity if for a lawful purpose. If a person can be clearly identified it is prudent to ask their consent to publish first. You cannot use photos of

children without written consent from a parent/guardian (not a grandparent) It is a good idea at events to have a poster and announcement saying publicity photos will be taken at this event and persons unwilling to participate should bring this to the attention of a trustee/organiser of the event.

Social Media/web events

If sharing events on CIO websites or social media it is a good idea to have a tick box on the hire agreement clearly consenting to you advertising the event or not.

CCTV Data

Will be added if a system is installed.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, staff and volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

The following are definitions of the terms used:

Data Controller - the trustees will collectively decide what personal information CIO will hold and how it will be held or used. The CIO is not required to appoint a DPO.

Act means the Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

Data Subject – the individual whose personal information is being held or processed by CIO for example a donor or hirer

'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.

Explicit consent is needed for processing "sensitive data", which includes:

- (a) Racial or ethnic origin of the data subject
- (b) Political opinions
- (c) Religious beliefs or other beliefs of a similar nature
- (d) Trade union membership
- (e) Physical or mental health or condition
- (f) Sexual orientation
- (g) Criminal record
- (h) Proceedings for any offence committed or alleged to have been committed

Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Data Protection Act 1998. As a micro business we do not need to register with the ICO but their website contains information and assistance of all matters pertaining to Data Protection Regulations.
Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.