Chieveley Recreation Centre

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 Chieveley Recreation Centre (CRC). This personal information must be collected and handled securely.

The Data Protection Act 2018 (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 CRC 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 with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The following are definitions of the terms used:

Data Controller - the trustees who collectively decide what personal information CRC will hold and how it will be held or used.

Act means the Data Protection Act 2018 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 CRC 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.

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.

Applying the Data Protection Act within the charity

CRC complies with its obligations under the Act by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

What are the Legal bases for processing your personal data?

1. To fulfil our **contracts for services** with you:
    a. To provide you with a booking service, the use of the hall and grounds;
    b. To procure your services as a supplier to the charity;
    c. To put on fireworks displays and other events and to provide tickets for admission;
    d. To facilitate coordination between successive users of facilities;
    e. To manage the 200 club and its operation, inform winners, seek subscriptions.
2. To fulfil a **legal obligation** or regulatory requirement:

   a. To make returns to the Charity Commission.
3. As necessary for **our own legitimate interests**:
   a. To contact hall executive members and trustees;
   b. To communicate matters related to the hall and grounds to the community of users;
   c. Making grant applications, managing grants and reporting to donors.
4. Based on **explicit consent**
   a. To promote up-coming events to those who have previously attended similar.

If you wish that we should not communicate with you any further, please inform us by email.

Sharing your personal data

Your personal data will be treated as confidential and will only be shared with CRC trustees, executives and users for purposes connected with the church under the above legal bases.

Your Rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

- The right to request a copy of your personal data which CRC holds about you;
- The right to request that CRC corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for CRC to retain such data;
- The right to withdraw your consent to the processing at any time;
- The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (where applicable).
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to object to the processing of personal data, (where applicable);
- The right to lodge a complaint with the Information Commissioners Office.

Responsibilities

CRC is the Data Controller under the Act, and is legally responsible for complying with 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:

a) Collection and use information fairly.

b) Specify the purposes for which information is used.

c) 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.

d) Ensure the quality of information used.

e) Ensure the rights of people about whom information is held, can be exercised under the Act.

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.

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 Act.

In case of any queries or questions in relation to this policy please contact the Secretary on villagehall@mychieveley.co.uk

Retention Policy

The aim is to retain personal data for only as long as is necessary:

Information Type	Event / Default Retention Period
Contact details for executive members, trustees	During their tenure + 1 year

Employee Records	During their tenure + 7 years
Contact details for those buying tickets for admission to events	13 months
Supplier records	Date of supply + 7 years
Contact details for those hiring facilities	Date of supply + 5 years
200 Club	During subscription
Charities Commission trustee records	In perpetuity
Minutes of meeting, memoranda, contracts, deeds	In perpetuity

Document Control

Version	Date	Content
0.2	20/6/18	Addition of document control, 3c
0.1	11/6/18	Initial draft for internal review

Procedures for Handling Data & Data Security

CRC 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 the information is held on paper, in a computer or recorded by some other means.

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. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the Act. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

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

Operational Guidance

Email:

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.

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

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 to 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.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

If you 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.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

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.

Always lock (password protect) your computer or laptop when left unattended.

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:

- 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 securely and will only be accessible to authorised volunteers or staff.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

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, will be kept indefinitely. If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

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 e.g. 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.

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.