shetland recreational trust
Registered Charity No: SC002179

Data Protection, Retention and Disposal Policy

Shetland Recreational Trust, Clickimin Leisure Complex, Lochside, Lerwick, Shetland, ZE1 0PJ

RELEASE: v1.0

DATE:05 November 2020

APPROVED BY:Trustees

OWNER: Assets & Business Support Dept

REVIEW DATE: November 2021

1. Introduction to Data Protection Legislation

1.1 Shetland Recreational Trust (SRT) is obliged to comply with the terms of the Data Protection Act 2018 (referred to in this policy as the "Data Protection Legislation") The Data Protection Legislation establishes a framework of rights and duties which are designed to safeguard personal data. This framework highlights the needs of an organization to collect and use personal data for business and other purposes against the right of individuals or data subjects (referred to as Individuals) to respect for the privacy of their personal details.

1.2 The Data Protection Legislation is underpinned by a set of data protection principles with the legal duty for enforcing compliance with the Data Protection Legislation falling to the Information Commissioner's Office (the ICO)

1.3 The Trust is committed to protecting the rights and privacy of employees and individuals in accordance with Data Protection Legislation.

1.4 Personal Data is defined as information relating to an identified or identifiable living individual and can be held in any format, electronic (including website and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

1.5 Failure to comply with the Data Protection Legislation could result in the prosecution not only of SRT but also of the individual responsible for the breach.

1.6 Data subjects may also sue for compensation for damage and any associated distress suffered where their rights have been infringed as a result of SRT breaching the Data Protection Legislation.

2. Scope

2.1. This policy applies to all SRT staff, all Trustees to the Board, contractors and suppliers appointed by SRT and any bodies or organisations working with SRT in a partnership agreement.

3. Equal Opportunities

3.1. SRT is committed to processing Personal data fairly and lawfully. Normally, the Trust will seek to obtain the consent of the individual to the processing of personal data. In relation to the processing of sensitive personal data (which is personal data relating to race/ethnic origins, political, religious or other similar beliefs, sexual life, medical condition, commission of any offence, criminal proceedings or sentences, or trade union membership), explicit consent to any processing will normally be obtained.

3.2. The Trust's key aim is to ensure that its policies and procedure do not create an unfair disadvantage for anyone, directly or indirectly.

4. Data Protection Principles

4.1. When processing personal data, the Trust will ensure that it complies at all times with the requirements of the Data Protection Legislation. This compliance will ensure all personal data that is collected is processed fairly and for lawful purposes. This personal data will also be stored safely and not disclosed to any other person unlawfully.

4.2. In order to achieve the requirements set out in section 1 of this policy, the Trust will comply in full with the data protection principles contained in the Data Protection Legislation in the following terms:

4.1.1 Personal data will be processed fairly and lawfully. Normally, the Trust will seek to obtain the consent of the individual to the processing of personal data. In relation to the processing of sensitive personal data (which is personal data relating to race/ethnic origins, political, religious or other similar beliefs, sexual life, medical condition, commission of any offence, criminal proceedings or sentences, or trade union membership), explicit consent to any processing will normally be obtained.

4.1.2 Personal data will be obtained for one or more specified and lawful purposes, and will not be further processed in any manner incompatible with that purpose or those purposes.

4.1.3 Personal data will be adequate, relevant and not excessive.

4.1.4 Personal data will be accurate and, where appropriate, kept up to date.

4.1.5 Personal data will not be retained for longer than is necessary.

4.1.6 Personal data will be processed in accordance with the rights of data subjects as defined by the Data Protection Legislation.

4.1.7 Appropriate measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.1.8 The Data Protection Legislation also covers the transferring of personal data to a third party that is located in a country or territory outside the European Union (EU)

5 Responsibilities for Compliance

5.1 Shetland Recreation Trust is the controller under the Data Protection Legislation. However, the following groups/individuals also have responsibilities for data protection compliance:

5.1.1 All Trustees.

5.1.2 The Chief Executive.

5.1.3 All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within their respective departments; and

5.1.4 Staff who process personal information as part of their duties.

5.2 The Chief Executive has overall responsibility for data protection matters and for reporting any serious data protection breaches to the ICO and to any affected individuals if required.

5.3 The Finance Manager is responsible for ensuring the required fees have been paid to the ICO and that the Trust maintains accurate and up to date records of our data processing activities.

6 The Rights of the Individual/Data Subject

6.1 Individuals have the following rights in relation to the processing of their personal data:

6.1.1 The right to receive information in relation to the Trust's processing of their personal data;

6.1.2 The right of access to a copy of the information comprising their personal data;

6.1.3 The right to object to processing of their personal data in certain circumstances, for example, for direct marketing;

6.1.4 The right to restrict the processing of their personal data for certain purposes;

6.1.5 The right to claim compensation for damages caused by a breach of the Data Protection Legislation;
6.1.6 The right in certain circumstances to have inaccurate personal data rectified;
6.1.7 The right to request that their personal data in a particular format for their own use; and
6.1.8 The right to request the ICO to assess whether any provision of the Data Protection Legislation has been contravened by the Trust.

6.2 Individuals have the right to request that the Trust specify whether personal data of which he or she is the subject is being processed by the Trust and to be given a description of the data, the purposes for which it is being processed and to whom it may be disclosed.

6.3 Individuals have the right to obtain a copy of any personal data held. To exercise this right a written request should be made to the Head of Assets and Business Support specifying the information sought. The Trust reserves the right to charge a fee for the information and, in accordance with Data Protection Legislation, the individual shall be provided within the 40 day period following the date on which the Trust is in receipt of both the written request and the fee. Where it is not possible to meet the one month time limit due to the request being manifestly unfounded or excessive, particularly in the case of repetitive requests, the Trust may extend the time limit in exceptional circumstances by two months, provided we inform the individual of the extension within one month.

6.4 Note that information requested which contains details relating to another individual will not normally be released (except in amended form) without that individual's consent. In addition, the Trust will not normally release any information relating to references given by the Trust on behalf of an Employee, management planning, information relating to negotiations with an Employee, e.g. over pay or any other information it is entitled to withhold in compliance with the Data Protection Legislation.

7 Privacy Statement

7.1 Before the Trust processes an individual's personal data, the individual must be given a "privacy statement" that provides information on how the Trust will use their personal data. Privacy statements will be included anywhere we request personal data from an individual, including on forms.

7.2 Privacy statements need to include:

7.2.1 Identity and contact details for the Trust;
7.2.2 The purposes and legal basis for processing personal data – if the Trust is processing personal data for legitimate purposes, details of what those are need to be included;
7.2.3 Details of any recipients of personal data, including details of any transfers out with the EU and what safeguards are in place for those transfers;
7.2.4 Details of how long the Trust will keep personal data;
7.2.5 Details of each of the individual's rights in relation to their personal data, including the right to complain to the ICO; and
7.2.6 Details of the consequences of the individual failing to provide their personal data if required under a contract or statute.

7.3 If the Trust receives an individual's personal data from a third party, then the individual must be given a privacy statement with the details above, and details of the types of personal data processed by the Trust and where the personal data came from. If the Trust knows that the

individual already has the privacy statement information or it would involve a disproportionate effort to provide the individual with a privacy statement then it need not provide one. Any decision not to provide a privacy statement must be authorised by the Chief Executive.

8 Consent

8.1 Where the Trust asks an individual for consent to process their personal data, the individual must be sign or submit a consent statement that includes of what they are consenting to, including different options for them to choose from where possible, and how they withdraw their consent.

8.2 The Data Protection Legislation states that it is not always appropriate to ask an individual for consent and consent may be invalid where:

8.2.1 The Trust would process the personal data even if consent is refused by relying on another legal basis under the Data Protection Legislation;
8.2.2 The consent is asked for as a precondition to a service; or
8.2.3 There is an "imbalance of power" between the Trust and the individual.

8.3 The Trust understands "consent" to mean that the individual has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

8.4 Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For special category personal data, explicit written consent of data subjects must be obtained unless an alternative legal basis for processing exists.

9 Disclosure of Data

9.1 This policy determines that personal data may be legitimately disclosed where one of the following conditions applies:

9.1.1 The individual has given their consent (e.g. an individual has consented to the Trust corresponding with a named third party).
9.1.2 Where the disclosure is in the legitimate interests of the Trust (e.g. disclosure to staff - personal data can be disclosed to other staff members if it is clear that those staff members require the personal data to enable them to perform their jobs).
9.1.3 Where the Trust is legally obliged to disclose the personal data (e.g. Statutory Agencies, Health and Safety returns, ethnic minority and disability monitoring).
9.1.4 Where disclosure of the personal data is required for the performance of a contract with the data subject.
9.1.5 Where disclosure of the personal data is necessary for the Trust to exercise its public functions and powers or perform a specific task in the public interest that is set out in law.

9.2 The Trust has a statutory obligation to provide certain types of personal data to third party organisations such as local authorities and the Department of Work and Pensions. In cases such as this, there is no requirement to gain consent from the data subject prior to disclosing the

requested personal data. However, where there is no statutory obligation to disclose personal data to a third party, then explicit consent will be sought by the Trust from the Data individual, unless there is a more appropriate legal basis under the Data Protection Legislation.

9.3 The Data Protection Legislation permits certain disclosures without consent so long as the information is requested for one or more of the purposes listed below. This type of information disclosure will only be accommodated providing the requests are supported by the appropriate legal documentation:

9.3.1. to safeguard national security;
9.3.2. prevention or detection of crime including the apprehension or prosecution of offenders;
9.3.3. assessment or collection of tax duty;
9.3.4. discharge of regulatory functions (includes health, safety and welfare of persons at work);
9.3.5. to prevent serious harm to a third party; and
9.3.6. to protect the vital interests of the individual, this refers to life and death situations

10 Data Subject Rights

10.1 Under the Data Protection Legislation, data subjects have the following rights with regards to their personal information held by the Trust:

10.1.1 The right to be informed about the collection and the use of their personal data.
10.1.2 The right to access personal data and supplementary information.
10.1.3 The right to have inaccurate personal data rectified, or completed if it is incomplete.
10.1.4 The right to erasure (to be forgotten) in certain circumstances.
10.1.5 The right to restrict processing in certain circumstances.
10.1.6 The right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services.
10.1.7 The right to object to processing in certain circumstances.
10.1.8 Rights in relation to automated decision making and profiling.
10.1.9 The right to withdraw consent at any time (where relevant).
10.1.10 The right to complain to the ICO.

10.2 Employees have the right to obtain a copy of any personal data held. To exercise this right a written request should be made to the Data Protection Officer (DPO) specifying the information sought. The Trust reserves the right to charge a fee for the information and, in accordance with Data Protection Legislation, shall be provided within the 40 day period following the date on which the Trust is in receipt of both the written request and the fee.

10.3 Where it is not possible to meet the one month time limit due to the request being manifestly unfounded or excessive, particularly in the case of repetitive requests, the Trust may extend the time limit in exceptional circumstances by two months, provided we inform the individual of the extension within one month.

10.4 All staff requests will be direct to their line manager. The line manager will then inform the DPO of the request by the staff member.

11 Retention and Disposal of Data

11.1 This section of the Policy has been developed to reflect an understanding of the administrative processes that give rise to records/file creation. This is independent of any particular format of record that might be historically created

11.2 The Data Protection Legislation does not set out any specific minimum or maximum period for retaining personal data. Instead, the Data Protection Legislation states personal data processed for any purpose shall not be kept longer than is necessary for its lawful purpose by the Trust.

11.3 It is therefore necessary to consider the reasons for collecting personal data and if the personal data should be retained when the relationship between the Trust and the individual ends.

11.4 Customers

11.4.1 In general, electronic customer records containing information about individual customers are kept 6 years following the end of their agreement as per the retention period unless any debt is left outstanding, information would then be kept indefinitely to allow reinstatement of the debt if another application is made and information would typically include name and address, date of entry and date of exit.

11.5 Staff

11.5.1 The Trust will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Data will normally only be held for a limited period of time. Where an Employee leaves the Trust, personal data will be kept only for such a period as may be necessary to protect the interests of the Trust and the Employee.

11.5.2 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. The Trust may keep a record of names of individuals that have applied for, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

11.5.3 The Trust will ensure at all times that personal data is disposed of in a way that protects the rights and privacy of data subjects. Typical methods employed by the Trust for disposal of data include the following:

- Shredding;
- Disposal as confidential waste; and
- Secure electronic deletion of data files.

12 Special Categories of Personal Data

12.1 As required under the Data Protection Act 2018, the Trust has assessed its purposes for processing special categories of personal data and shall ensure compliance with the data protection principles as follows:

12.1.1 Lawfulness, fairness and transparency – The Trust has undertaken a data audit and maintains a record of its processing of special categories of personal data, which includes an assessment on the legal basis and special condition under which such data is processed. The Trust is satisfied that we have a legal basis and special condition for

holding the relevant special categories of personal data, which is referred to within the Trust's Privacy Statements.

12.1.2 Purpose limitation – The Trust's purposes for collecting special categories of personal data are specified within the Trust's Privacy Statements.

12.1.3 Data Minimisation – The Trust has accessed the datasets held and has guidance in place to ensure that only the special categories of personal data which are necessary for our purposes are held.

12.1.4 Accuracy – The Trust will continually check for accuracy and take steps to correct any inaccuracies, should they arise.

12.1.5 Storage limitation – The Trust follows the retention and disposal section of this policy and has assessed appropriate retention periods for special categories of personal data.

12.1.6 Integrity and confidentiality – The Trust has procedures in place to ensure the security of special categories of personal data and will have additional security measures for such data, where appropriate.

13 Data Security

13.1 There is a duty placed on the Trust by the Data Protection Legislation to ensure there is appropriate security to prevent personal data being accidentally or deliberately compromised.

13.2 All staff, Trustees and appointed contractors are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to un-authorised third parties. Only authorised staff, Trustees and appointed contractors can access, alter, disclose or destroy personal data within the scope of their authority.

13.3 Personnel files will be stored in locked cabinets, and access to computerised records will be password protected. Staff should also ensure any personal data displayed on a PC screen cannot be viewed by an un-authorised third party either in the workplace or when using any form of digital media device in a public place.

13.4 In terms of minimising risks associated with breaches of the Data Protection Legislation through lapses in personal IT security, staff with access to personal data should always ensure their PC is 'locked' if they need to leave their desk.

13.5 Any misuse of personal data or breaches of data security by staff, Trustees or contractors may result in disciplinary or legal action being taken against the individual.

13.6 Significant data breaches covered by the Data Protection Legislation will be reported at the earliest opportunity to the respective Governing Body. This is important in order for the Trust to comply with the Data Protection Legislation, which sets down a statutory time limit for reporting certain data protection breaches to the ICO and affected individuals within 72 hours of the Trust becoming aware of the breach.

14 Risk Management and Audit

14.1 Not only could a data breach cause adverse publicity for the Trust but, if an employee is the person responsible for the infringement, the Employee could be the subject of a personal criminal prosecution and liable to a fine. It is important to keep the penalties in perspective, however. If the Employee follows the advice given below and takes sensible and reasonable precautions to protect information in the Employee's case there should be few, if any, problems.

14.1.1 Observe to the letter any instruction or guidelines issued by the Trust in relation to data protection and your work.

14.1.2 Observe the data protection principles set out in the Data Protection Legislation at all times.

14.1.3 Take confidentiality and security seriously whether you consider the information to be sensitive or not. In particular:-

- do not disclose your password;
- change your password regularly;
- do not gossip about Trust data;
- do not leave Trust data in the street, on the ferry, or on the bus etc.;
- do not take computer scrap paper home; and
- do not allow unauthorised use of computer equipment issued by the Trust.

14.2 The Trust aims to mitigate the risk of potential financial penalties and compensation payments through failure to adhere to the Data Protection Legislation through the provision of training to staff on data protection issues as detailed in Section 12 of this policy. The Trust will also review this policy and the associated procedures on a regular basis to ensure that they meet all legislative and regulatory requirements and best practice guidance. In addition, a review of the personal data held by the Trust will be carried out as part of the Internal Audit plan to ensure ongoing compliance with the provisions of the Data Protection Legislation.

14.3 Internal audit procedures will form an important part of establishing and sustaining good data protection practices. The Trust will review the personal data it processes and collects and assess this against the data protection principles as listed in Section 4 of this policy. This will inform the review of our action plan to ensure compliance with this policy.

14.4 The Trust undertake self-assessment to periodically check our compliance with the Data Protection Legislation; our Data Protection Policy and guidance, regulatory and good practice guidance; our registration with the ICO; our working practices in the collection, processing and storage of personal data.

14.5 Data protection issues will be considered as part of the Risk Management Strategy, and if assessed as a priority risk area the commitment of resources will be considered to attend to the controls to mitigate these risks.

15 Training

15.1 All individuals permitted to access personal data in line with their work duties will be trained in data protection following the implementation of this Data Protection, Retention and Disposal Policy. All individuals with access to personal data on or behalf of the Trust, must agree to undertake any relevant training that may be deemed appropriate.

15.2 Data Protection training will form part of the Induction training of new staff members. A copy of this Data Protection, Retention and Disposal Policy will be provided to all staff members (including Agency Staff) and Governing Body members.

shetland recreational trust
Registered Charity No: SC002179

Privacy Notice for Website/Customers

Shetland Recreational Trust, Clickimin Leisure Complex, Lochside, Lerwick, Shetland, ZE1 0PJ

RELEASE: v1

DATE APPROVED: November 2020

REVIEW DATE: November 2023

1. What we need

1.1 Shetland Recreational Trust (SRT) is a charitable organisation and has Charitable status granted by the Inland Revenue in Scotland. The Scottish Charity Registration number is SC002179.

1.2 Shetland Recreational Trust will be a "controller" of the personal information that you provide to us unless otherwise stated.

1.3 This section lists out the types of personal data that the controller will collect from individuals. It is only strictly necessary to set out these categories when collecting personal data from a third party. However, if the Trust has one privacy notice for a form/application that allows parents to provide personal data on behalf of their children then it is useful for the categories to be included.

1.4 If the Trust collects personal data of which it is the controller and then discloses such personal data to a third party (for example, a SGB) and that third party becomes the controller of the disclosed personal data, we would recommend that the privacy notice clearly states this.

1.5 Customers' personal data:

1.5.1 When you register as a customer of Shetland Recreational Trust or purchase a subscription (including if you are registering or renewing on behalf of a child under the age of 16, we will ask you for the following personal information:

- Name, address, email address, date of birth, contact numbers etc.
- Subscription type – for example, standard adult, senior junior, etc.
- Payment details – bank account number, sort code, card details, etc.
- Equality information – for example, gender, disability, etc.

2 Why we need your personal information – contractual purposes

2.1 Customers' personal data:

2.1.1 We need to collect our customers' personal information so that we can manage your bookings and subscriptions We will use our customer's personal information to:

- Set up your unique customer booking account which also allows for online bookings
- Send you customer communications if opted in, by agreed communication methods, in relation to essential customer services, including but not limited to, booking confirmations, payment confirmations, price increases, promotional offers etc.

2.2 If you do not provide us with all of the personal information that we need to collect then this may affect our ability to offer the above customers services.

3 Why we need your personal information – legitimate purposes

3.1 Customers' personal data:

3.1.1 We also process our customers' personal information in pursuit of our legitimate interests to:

- Promote and encourage participation in a variety of activities by sending customers' communications and booking information for upcoming activities and events. Our activities and events may be filmed or photographed and your personal information may also be used in images captured from our activities and events, which we use for promotional, education and development purposes;
- Provide activities by accepting and managing bookings for our facilities and checking your personal information to ensure you are eligible for the facility or activity;
- Monitor and develop participation in activities by monitoring customers' engagement and participation and inviting our members to participate in surveys for researching and development purposes;
- Respond to and communicate with members regarding your questions, comments, support needs or complaints, concerns or allegations made. We will use your personal information to investigate your complaint, to suspend subscriptions, take disciplinary action, etc.

3.2 Where we process your personal information in pursuit of our legitimate interests, you have the right to object to us using your personal information for the above purposes. If you wish to object to any of the above processing, please contact us on mail@srt.org.uk If we agree and comply with your objection, this may affect our ability to undertake the tasks above for the benefit of you as a member

4 Other uses of your personal information

4.1 We may ask you if we can process your personal information for additional purposes. Where we do so, we will provide you with an additional privacy notice with information on how we will use your information for these additional purposes.

5 Who we share your personal information with

5.1 If your personal information is included in any images or videos taken by us at our activities and events, we may share this for promotional and/or journalistic purposes.

5.2 We may be required to share personal information with statutory or regulatory authorities and organisations to comply with statutory obligations. Such organisations include the Health & Safety Executive, Disclosure Scotland, and Police Scotland for the purposes of safeguarding children.

5.3 We may also share personal information with our professional and legal advisors for the purposes of taking advice.

5.4 Shetland Recreational Trust employs third party suppliers to provide services, including direct debit banking. These suppliers may process personal information on our behalf as "processors" and are subjects to written contractual conditions to only process that personal information under our instructions and protect it.

5.5 In the event that we do share personal information with external third parties, we will only share such personal information strictly required for the specific purposes and take reasonable steps to ensure that recipients shall only process the disclosed personal information in accordance with those purposes.

6 How we protect your personal information

6.1 Your personal information is stored on our electronic filing system and our servers based in the UK/EU, and is accessed by our employees for the purposes set out above.

7 How long we keep your personal information

7.1 We will only keep your personal information for as long as necessary to provide you with customer services, Unless you ask us not to, we will review and possibly delete your personal information where you have not actively made a booking with us for two years.

7.2 We will keep certain personal information of customers for longer in order to confirm your identity, when you were a customer of Shetland Recreational Trust and for how long. We need to do this to keep a register of customers in the event of a claim against the Shetland Recreational Trust.

8 Your Rights

8.1 You can exercise any of the following rights by writing to us at mail@srt.org.uk

8.2 Your rights in relation to your personal information are:

- You have the right to request access to the personal information that we hold about you my making a "subject access request"
- If you believe that any of your personal information is inaccurate or incomplete, you have a right to request that we correct or complete your personal information
- You have the right to request that we restrict the processing of your personal information for specific purposes
- If you wish us to delete your personal information, you may request that we do so

8.3 Any requests received by Shetland Recreational Trust will be considered under applicable Data Protection Legislation. If you remain dissatisfied, you have a right to raise a complaint with the Information Commissioner's Office at www.ico.org.uk