Shetland Recreational Trust

# Data Protection, Retention & Disposal Policy

Scope: All SRT employees and third parties providing services to the Trust.

Aim: This policy is part of a framework of policies for protecting personal data, safeguarding individual privacy, and ensuring lawful and fair processing in line with the Data Protection Act 2018 and UK General Data Protection Regulations (UK GDPR).

V 2.0

Approved: October 2024

## 1. Introduction to Data Protection Legislation

1.1. Shetland Recreational Trust (SRT) is required to comply with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), or EU GDPR where applicable (collectively referred to as the "Data Protection Legislation"). This legislation creates a framework of rights and responsibilities designed to protect personal data, balancing the need for organisations to collect and use personal data with the rights of individuals (referred to as "data subjects" or "individuals") to have their privacy respected.

1.2. The Data Protection Legislation is built on key principles, with the Information Commissioner's Office (ICO) serving as the authority responsible for enforcing compliance.

1.3. SRT is committed to safeguarding the rights and privacy of employees and individuals in accordance with the Data Protection Legislation.

1.4. "Personal Data" is defined as information related to an identified or identifiable living person, which may be stored in any format (e.g., electronic, paper, photographic), as long as the individual's data can be readily extracted.

1.5. Failure to comply with the Data Protection Legislation could result in prosecution of both SRT and any individual responsible for the breach.

1.6. Data subjects can also seek compensation for damages and associated distress caused by SRT's violation of the Data Protection Legislation.

## 2. Scope

2.1. This policy applies to all SRT staff, Board Trustees, contractors, suppliers, and any organisations or bodies working with SRT under partnership agreements.

2.2. This policy should be read in conjunction with the:

- SIC Information Security Policy
- SRT Addendum to the SIC Information Security Policy
- Cardholder Data Security Guidance and Compliance Agreement

## 3. Equal Opportunities

3.1. SRT is committed to processing personal data fairly and lawfully. Generally, SRT will seek the individual's consent before processing their personal data. For sensitive personal data (e.g., data related to race/ethnic origin, political or religious beliefs, sexual orientation, health, criminal records, or trade union membership), explicit consent will typically be obtained.

3.2. SRT aims to ensure that its policies and procedures do not create any unfair disadvantages for individuals, either directly or indirectly.

## 4. Data Protection Principles

4.1. When processing personal data, SRT will comply with the requirements of the Data Protection Legislation to ensure that all personal data is processed fairly, lawfully, stored securely, and not unlawfully disclosed.

4.2. To meet these obligations, SRT will adhere to the following data protection principles:

- Personal data will be processed lawfully and fairly, typically with the individual's consent.
- Data will only be collected for specific, lawful purposes and not further processed in incompatible ways.
- Data will be adequate, relevant, and not excessive.
- Data will be accurate and kept up-to-date where necessary.
- Data will not be kept longer than necessary.
- Data will be processed in line with the rights of data subjects.
- Appropriate measures will be taken to protect against unauthorised or unlawful processing, accidental loss, or damage.
- Transfers of personal data outside the UK will comply with legal requirements.

## 5. Responsibilities for Compliance

5.1. SRT is the data controller under the Data Protection Legislation. The following roles also have specific responsibilities:

- All Trustees.
- The Chief Executive.
- Managers and supervisors responsible for promoting good data-handling practices within their teams.
- Staff who handle personal information as part of their job responsibilities.

5.2. The Chief Executive holds overall responsibility for data protection, acting as the Data Protection Officer (DPO) including reporting serious breaches to the ICO and affected individuals, within 72 hours of the breach being identified, in line with legislation.

## 6. Individual/Data Subject Rights

6.1. Data subjects have the following rights regarding the processing of their personal data:

- The right to be informed about the Trust's data processing activities.
- The right to access their personal data.
- The right to object to data processing in certain situations, such as direct marketing.
- The right to restrict data processing in specific circumstances.

- The right to seek compensation for damages caused by data protection breaches.
- The right to have inaccurate personal data corrected.
- The right to request their personal data in a structured format.
- The right to request an ICO assessment of any potential breaches of the legislation.

6.2. Individuals can request details about whether SRT is processing their personal data, the purposes for such processing, and to whom the data may be disclosed.

6.3. To request a copy of their personal data, individuals should submit a written request to the Chief Executive. SRT must provide the requested information within one month, though it may take longer in exceptional circumstances.

6.4. Requests involving another individual's personal data will not be released without consent unless legally required. The Trust may also withhold certain data (e.g., employee references or management planning data) as allowed by the legislation.

## 7. Privacy Statement

7.1. Before processing an individual's personal data, SRT will provide a "privacy statement" outlining how their data will be used. This will be included on any forms requesting personal data. SRT uses two different privacy statements, for employees and workers, and for customers.

7.2. Privacy statements will include:

- SRT's identity and contact information.
- The purposes and legal basis for data processing.
- Information about any data recipients, including data transfers outside the UK.
- Data retention periods.
- Information about the individual's rights, including the right to complain to the ICO.

7.3. If personal data is received from a third party, a privacy statement will be provided to the individual unless they already have the information or providing it would require disproportionate effort.

## 8. Consent

8.1. Where consent is required, under GDPR, it must be freely given, specific, informed and unambiguous.

8.2. When SRT seeks consent to process personal data, individuals will be asked to sign a consent form. They will be informed that they may withdraw consent at any time, including how to do so.

8.3. Consent may not be appropriate if:

- SRT would process the data regardless of consent.
- Consent is a precondition for service.
- There is an "imbalance of power" between SRT and the individual.

8.4. Consent must be freely given, informed, and not obtained under pressure. It cannot be assumed from a lack of response.

## 9. Special Categories of Personal Data

9.1. As required by the Data Protection Act 2018, the Trust has assessed its reasons for processing special categories of personal data and ensures compliance with data protection principles:

- **Lawfulness, Fairness, and Transparency**: The Trust has undertaken a data audit and maintains records of its processing of special categories of personal data, assessing the legal basis and conditions for processing such data. These legal bases are reflected in the Trust's Privacy Statements.
- **Purpose Limitation**: The purposes for collecting special categories of personal data are specified in the Trust's Privacy Statements.
- **Data Minimisation**: The Trust has guidelines in place to ensure that only necessary special categories of personal data are held.
- **Accuracy**: The Trust will continually check for accuracy and take steps to correct inaccuracies when they arise.
- **Storage Limitation**: The Trust follows the retention and disposal policies set out in this document and has defined appropriate retention periods for special categories of personal data.
- **Integrity and Confidentiality**: The Trust has put in place procedures to ensure the security of special categories of personal data, with additional security measures where appropriate.

## 10. Disclosure of Data

10.1. Personal data may be disclosed if:

- The individual has given consent.
- Disclosure is in the legitimate interests of SRT (e.g., to enable staff to perform their jobs).
- SRT is legally required to disclose the data.
- Disclosure is required for contractual purposes.

10.2. Some disclosures (e.g., to statutory agencies) do not require individual consent. However, if there is no legal obligation, explicit consent will be sought.

## 11. Data Subject Rights

11.1. Data subjects have additional rights under the legislation, including the right to erasure ("right to be forgotten") and the right to data portability.

11.2. To request access to personal data, employees should make a written request to the Chief Executive, who is the DPO.

## 12. Retention and Disposal of Data

12.1. SRT will retain personal data only as long as necessary for its lawful purposes and will comply with all legal and regulatory requirements to retain data.

12.2. No data is created or retained without a good business reason, or a legal or regulatory requirement.

12.3. Appropriate resources will be allocated to ensure the security and appropriate disposal of data, and roles and responsibilities have been identified to manage data retention and disposal.

12.4. The Chief Executive, acting as Data Protection Officer (DPO) has overall responsibility, however day to day responsibilities are as follows:

- **Employee Records** – People Managers, Supervisors and the Financial Services Officer.
- **Customer Data** – Centre Managers, Customer Services Team Leader and the Operations Support Officers.
- **Financial Records** – Finance Manager, Finance Officer, Finance/Payroll Officer, Assistant Accountant, Operations Support Officers, and Centre staff.
- **Health & Safety** – Centre Managers and the Technical Services Manager.
- **Adult & Child Safeguarding** – Adult and Child Safeguarding Officers.
- **Miscellaneous** – All of the above, Marketing Officer, and any other relevant members of staff.

12.5. Our data retention schedule is attached as Appendix 1 and is a live document which will be kept under review and updated as required.

## 13. Data Security

13.1. All employees **must** adhere to the:

- Data Protection, Retention and Disposal Policy
- SIC Information Security Policy
- SRT Addendum to the SIC Information Security Policy
- Cardholder Data Security Guidance and Compliance Agreement

13.2. All staff, trustees, and contractors must ensure that personal data is kept secure and not disclosed to unauthorised third parties. Only authorised personnel may access, alter, disclose, or destroy personal data within their scope of authority.

13.3. Misuse of personal data or breaches of data security by staff, trustees, or contractors may result in disciplinary or legal action.

## 14. Training

14.1. All individuals with access to personal data as part of their duties will undergo data protection training. This training will ensure individuals understand their responsibilities under the relevant policies.

14.2. Data protection training is mandatory as part of the induction process for new staff members. A copy of all relevant policies are provided within the Employee Handbook.

# Customer Privacy Statement

## 1. Introduction

1.1. Shetland Recreational Trust (SRT) is committed to protecting your privacy and ensuring the security of your personal data in compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and, where applicable, the **EU GDPR**. This privacy statement explains how we collect, use, store, and protect your data and outlines your rights in relation to your personal information.

## 2. Data Controller

2.1. SRT, registered as a charity (SC002179), is the data controller responsible for determining the purposes and means of processing personal data.

## 3. Personal Data We Collect

3.1. We may collect the following categories of personal data:

- **Identity data:** Names, titles, dates of birth.
- **Contact details:** Email addresses, phone numbers, physical addresses.
- **Financial data:** Bank account details for membership payments.
- **Usage data:** Information on how you use our website and services.
- **Health data:** Where required, information related to medical conditions or health, collected with explicit consent for the purposes of delivering relevant services (e.g., fitness classes).

## 4. Lawful Basis for Processing

4.1. We process your data under the following lawful bases:

- **Consent**: For certain activities such as marketing communications.
- **Contractual necessity:** To fulfil our obligations when you enter into a contract with us (e.g., MORE4life memberships).
- **Legal obligation**: To comply with applicable laws and regulatory requirements.
- **Legitimate interests**: To provide, operate, and improve our services.

## 5. How We Use Your Data

5.1. Your personal data will be used for the following purposes:

- To provide and manage services (e.g., memberships, bookings, and facility usage).
- To communicate with you regarding services, changes, or promotional offers (with your consent).
- To improve our website and services by analysing usage patterns.
- To comply with legal obligations (e.g., maintaining records for tax purposes).

## 6. Data Subject Rights

6.1. As a data subject, you have the following right:

- **Right to access**: You may request a copy of the personal data we hold about you.
- **Right to rectification**: You can request corrections to your personal data if it is inaccurate or incomplete.
- **Right to erasure**: You have the right to request deletion of your data, where applicable, under the "right to be forgotten."

- **Right to restrict processing**: You can request restrictions on how we process your data in certain circumstances.
- **Right to data portability**: You may request your data in a structured, commonly used format to transfer it to another service.
- **Right to object**: You have the right to object to the processing of your data for specific purposes, such as direct marketing.
- **Right to withdraw consent**: If processing is based on consent, you may withdraw this at any time.
- **Right to lodge a complaint**: If you believe your data rights have been violated, you have the right to file a complaint with the Information Commissioner's Office (ICO).

## 7. How We Protect Your Data

7.1. We implement appropriate technical and organisational measure to safeguard your personal data from unauthorised access, disclosure, alteration, or destruction. These include:

- Encryption of sensitive data.
- Restricted access to personal data.
- Regular reviews of data protection measures and staff training on data security.

## 8. Data Retention

8.1. We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected or to comply with legal obligations. For example:

| Data Type | Retention Period | Reason for Retention | Disposal Method |
|---|---|---|---|
| Contact information and booking history | 6 years after contract ends | Legal and financial records, potential disputes | Secure shredding (paper), permanent deletion (digital) |
| Means tested information | Until membership is confirmed | Internal records | Secure shredding (paper), permanent deletion (digital) |
| Payment information (excluding card details) | 6 years after transaction | Financial record-keeping, potential disputes | Secure shredding (paper), permanent deletion (digital) |
| Banning Reports | 1 year after the ban ends | Internal records, potential legal claims | Secure shredding (paper), permanent deletion (digital) |
| Customer Cardholder data (terminals) | Until transaction is completed | PCI DSS compliance | Secure shredding (paper), never store digitally |
| Customer Cardholder data (RCP) | Until membership is cancelled | PCI DSS compliance | Never store on paper, permanent deletion (digital) by customer |
| Customer Cardholder data (Wallet) | Until customer removes | PCI DSS compliance | Never store on paper, permanent deletion (digital) by customer |
| Customer Direct Debit Mandates and other related communications | 6 years after the last payment or cancellation | Compliance with financial regulations, reconciliation, audit, to verify authorisation and address disputes or claims | Secure shredding (paper), permanent deletion (digital) |

## 9. Sharing Your Data

9.1. We will not share your personal data with third parties without your consent, except where required by law or to fulfil contractual obligations. We may share you data with:

- Service providers working on our behalf (e.g., payment processors, IT service providers).
- Government bodies or law enforcement when required to comply with legal obligations.
- In cases of international data transfers, we will ensure adequate safeguards are in place, such as Standard Contractual Clauses (SCCs) or adequacy decisions.

## 10. International Data Transfers

10.1. Where your data is transferred outside the UK or EEA, we ensure it is protected by appropriate safeguards such as:

- Standard Contractual Clauses (SCCs) approved by the UK or European Commission.
- Transfers to countries with an adequacy decision by the European Commission or UK Government.

## 11. Changes to this Privacy Statement

11.1. We may update this statement from time to time to reflect changes in our practices or legal obligations. Any significant changes will be communicated via email or our website. Please review this statement periodically to ensure you are informed about how we protect your data.

## 12. Contact Us

12.1. If you have any questions or concerns about this privacy statement or your data rights, please contact us:

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

**Email:** mail@srt.org.uk

**Phone:** (01595) 741000

12.2. If you believe that your data protection rights have been violated, you can also contact the **Information Commissioner's Office (ICO)** at www.ico.org.uk.