GDPR Compliance Statement

Draft version 0.1 - for review

1. What is the GDPR

The EU General Data Protection Regulation ("GDPR") came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. At the present time, despite the UK having exited the European Union, organisations in the UK are still required to be compliance with this regulation.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

2. Shildon Railway Institute's Commitment

Shildon Railway Institute is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have a robust and effective data protection program in place and recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

Shildon Railway Institute is dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the GDPR Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

Our preparation has included: -

- **Execution of an Information Audit** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed. This is captured in a Data Resource Spreadsheet for our organisation.

- **Definition and Implementation of Policies & Procedures** - producing new, and revising existing data protection policies and procedures, so as to meet the requirements and standards of the GDPR and any other current data protection laws, including:
    - **Data Protection** – our main policy and procedure document for data protection has been replaced with new documentation to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities.

    - **Data Retention & Erasure** – we have reviewed and updated our data retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have data erasure procedures in place and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
    - **Data Breaches** – our breach procedure ensures that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time in line with ICO guidance.
    - **International Data Transfers & Third-Party Disclosures** – Shildon Railway Institute does not store or transfers personal information outside the EU.

- **Subject Access Request (SAR)** – A member, customer or employee has the right to access information kept about them by Shildon Railway Institute, including but not limited to: member's details, share holding details, customer booking queries and details, customer ticket purchase records, customer purchase records, personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee. The Secretary of the Management Committee is responsible for dealing with data subject access requests. We promise to accommodate the revised 30-day timeframe for providing the requested information, subject to the correct circumstances and are aware of the circumstances when we can extend the time limit to respond to a request. We also understand when to consider if a request includes information regarding others and any implications this may have.

- **Legal Basis for Processing** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met. See below for a summary of processing activities:

Theme	Purpose	Data Cluster	Data Items
Human Resources	So we can understand who works for us, when, how long, how and when they are paid	Employee data	Names, addresses, salary, bank details, sickness figures, working hours, shift rota
Membership Register	So we can understand who our shareholding members and service subscribers are	Member data	Names, addresses, contact phone numbers, contact email addresses, membership class, shareholding, joining dates, renewal information, membership statuses, contact permissions
Event Ticket Purchase Data	So we can understand who has made online purchases of tickets (physical purchases offline are anonymous) and can resolve disputes and issues with the customer	Purchase data	Names, addresses, contact phone number, contact email address, event data, ticket volume data

Theme	Purpose	Data Cluster	Data Items
Online Product Order Data	So we can understand who has made online purchases of our merchandise, how to fulfil them, and can resolve disputes and issues with the customer	Purchase data	Names, addresses, email addresses, telephone contact numbers, product name, product quantity, payment method (but not specific payment method details)
Hall Booking Online Enquiries	So we can understand who would like to book either the main hall, the lounge or the MacNay room	Order enquries	Customer name, room required, desired booking date, email address, contact phone number, event details, no of guests.

- **Privacy Notice/Policy** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

- **Obtaining Consent** – we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- **Direct Marketing** – Shildon Railway Institute does issue direct marketing communications to members where that member has give us permission to do so at the time of becoming a member, renewing membership or signing up for marketing communications via our website. We have a robust procedure for persons receiving direct marketing messages to withdraw permission to do so.

- **Data Protection Impact Assessments (DPIA)** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we are revising our documentation processes that record each assessment, this will allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- **Processor Agreements** – where we use any third-party to process personal information on our behalf (i.e. web hosting, email handling, ticket sales etc.), every care has been taken to ensure all parties are compliant with the GDPR and are aligned to Shildon Railway Institute's ongoing commitment. These measures have included the selection of trusted partners with a good track record for data privacy compliance, initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

- **Special Categories Data** - Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, or is provided directly by an employee with the right to modify or remove consent being clearly signposted.

3. Correction of data

Shildon Railway Institute has a system in place that enables members, customers and employees to check their personal information on a regular basis so that they can correct, delete or update

any data. If a person becomes aware that Shildon Railway Institute holds any inaccurate, irrelevant or out-of-date information about them, they must notify the Secretary of the Management Committee immediately and provide any necessary corrections and/or updates to the information.

4. Monitoring

Shildon Railway Institute may monitor member data through its annual renewals process. It may also monitor employees and customers activity by means including, but not limited to, recording employees' activities on CCTV. Where this is the case, Shildon Railway Institute will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. This is primarily done to ensure security of the building and safeguarding of our staff, volunteers and customers and members. Employees affected will usually be entitled to be given any data that has been collected about him/her. Shildon Railway Institute will not retain such data for any longer than is necessary.

5. Employees' Obligations Regarding Personal Information

Employees, management committee members and volunteers whom handle person data must ensure that:

- The information is accurate and up to date, insofar as it is practicable to do so;
- The use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- The information is secure.
- Uses password-protected software and non-personal email accounts for the transmission and receipt of emails sent or received in respect of carrying out Shildon Railway Institute's business;
- Locks files containing personal data in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This will involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of personal information will need to be confidentially shredded or permanently destroyed by other means.

If, in the unlikely event, an employee is required to disclose personal data to any other country, then they must ensure first that there are adequate safeguards for the protection of data in the host country.

An employee, management committee member or volunteer must not take any personal information away from Shildon Railway Institute's premises without the prior consent of the Management Committee.

If an employee is in any doubt about what about what they may or may not do with personal information, they should seek advice from the Management Committee.

6. Consequences of Non-Compliance

All employees, management committee members and volunteers are under an obligation to ensure that they comply with the data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this document may result in the person incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal and or expulsion from position.

7. Taking Records off Site

An employee or member of the Management Committee may only take membership data records off site with agreement of the management committee, where they feel that the reason is appropriate and the risks of doing so are fully mitigated. Records or information will never be sent offsite by email, particularly to personal email accounts.

Any employee or member of the Management Committee taking records off site must ensure that they do not leave their laptop, other device or any hard copies of membership records unattended. They must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

8. Loss of Data

Shildon Railway Institute takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- Restricted access to files and folders, with a view of all personal data is accessed on a 'need to know' basis
- Explicit guidance regarding the security marking of such previously mentioned data
- An appointed CISO (Chief Information Security Officer), being the serving Secretary of Shildon Railway Institute Management Committee to review compliance and best practice surrounding all aspects of cyber security
- Being accountable for reporting any breaches to the SIRO (Senior Information Risk Owner), being the serving Chairperson of the Shildon Railway Institute Management Committee.

Should there be any incident occur where there is loss or potential loss of personal or special personal data, it should be reported to the CISO and SIRO (see above)

9. Compliance

- General Data Protection Regulation 2018
- Data Protection Act 1998

10. Definitions/Abbreviations

- GDPR General Data Protection Regulation
- ICO Information Commissioners Office

11. Supporting Information

11. Amendment Record

Date	Section or Paragraph Amended	Amendment Details
27 Feb 2023	Whole Document	First draft issue for review and comment