DATA PROTECTION POLICY

Purpose

The purpose of this policy is to ensure that the Trust provides appropriate protection to the storage and use of personal data held.

The policy has been reviewed and updated to align with the new General Data Protection Regulations (GDPR) 2018.

Policy statement

The Mersey Rivers Trust (MRT) has a seven-point plan to ensure that its current practice is strengthened and complies with the intent as well as the letter of the new regulations:

1. Define who is responsible?
2. Know what data we hold
3. Update our privacy notices (Required for sign-up on CaBA and RT mailing lists)
4. Dealing with subject access requests
5. Extra protection for children
6. Reporting data breaches
7. Data protection by design

The following sections will deal with each of these parts of the plan.

Who is responsible?

The main roles identified with respect to the control of data are:

Data Controller: The Trustees are ultimately responsible for the Trust's management of data and fulfil the role of "Data Controller". The Data Protection Policy will be reviewed annually by the Trust Director and Trustees and will be updated with any issues or risks to ensure that it is fit for purpose and that the purpose for collecting, storing and processing personal data is still required for the Trust's work.

Data Processor. This is the Trust Director, whose main responsibilities are to ensure that any processing of personal data within the Trust is done in accordance with the regulations and that data protection is built in at the design stage of any project rather than added in at the end.

Back-up of databases and security. This is the responsibility of the Data Processor. From time to time individuals will ask informally to be added to contact databases. These requests need to be sent to the lead contact for the database (administrator). This will ensure that we audit the permission process and that the details are added to the correct database.

We know what data we hold & have created a data inventory

The Trust has audited its data holdings; identified the main sources of data and generated a data inventory (spreadsheet). The inventory identifies where that data has come from; when it was collected

and any third parties with whom the data has been shared. The Trust believes that it has identified all sources of personal data retained by Trust staff, however, it is possible that legacy data will be uncovered in the future, if this happens the data will be deleted.

Review privacy notices and how we ask for consent and remove data on request

The Data Processor is responsible for the review of the Trust's privacy notices and how we ask for consent to ensure that the Trust continues to follow best practice. The Data Inventory will be used to identify and remove personal data on request.

Build in extra protection for children

The Trust has only collected data from adults and it has not knowingly collected data from children. Should the Trust plan to collect personal data from children it will review its procedures and build in suitable protection as required.

Design in data protection at the start of a project

Data protection will be incorporated into the initial risk assessment for all projects to ensure that it is designed into each project. This will be project specific and the responsibility of the project manager.

General principles for the collection and use of personal data

1 Processed fairly and lawfully.

2 Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with the purpose or those purposes.

3 Adequate, relevant and not excessive in relation to the purpose(s)for which it is held.

4 Accurate and, where necessary, kept up to date.

5 Held no longer than is necessary for the specified purpose(s).

6 Processed in accordance with the rights of the data subjects.

7 Held securely, with appropriate technical and organisational measures taken to prevent unauthorised or unlawful processing of personal data, and to prevent accidental loss or destruction of, or damage to, personal data.

Fair Processing

All personal data processed will meet one of the conditions below:

(a) The data subject has given consent explicitly, where the purpose is obvious (e.g. gift aid).

(b) The personal information is related to the individual's professional interest in a project. This covers work emails, addresses and telephone numbers but NOT private details.

(c) The processing is necessary to carry out a contract (e.g. environmental advice given to an individual).

(d) It is needed to process the data in order to comply with a legal obligation (e.g. Inland Revenue notification).

(e) It is necessary to protect the vital interests of the data subject (e.g. payroll).

(f) It is necessary for the administration of justice or for government or other functions of a public nature (e.g. claim for loss of wages).

Sensitive Personal Data

This will not be collected or processed by the Trust. If it is collected, the prior express consent of the data subject will be obtained. Sensitive personal data is information relating to:

(a) Racial or ethnic origin.

(b) Religious beliefs or similar.

(c) Trade union membership.

(d) Physical or mental health or condition.

(e) Sexual life.

(f) Commission or alleged commission of any offence.

(g) Any proceedings for any offences committed or allegedly committed by any data subject, the disposal of such proceedings or the Court's sentence in any such proceedings.

Protection of Personal Data

(a) Physical protection

The Trust's employees are required to effect and maintain security protection on all computers in accordance with the MRT IT Policy. With home/office locations, there are self-defining safeguards against theft of, inter alia, computers and hard copy files. The Trust does not encrypt files transmitted by email, and accordingly will not transmit any sensitive personal information by email. Contact details may be transmitted electronically within the Trust from time to time.

(b) Confidentiality undertakings

All employees have a confidentiality clause within their contracts of employment. Personal data is largely incidental to the business advice given. The confidentiality and personal data obligations are periodically reinforced at staff meetings.

Any external fundraising agreements or consultation responses will incorporate a clause making the confidentiality and data protection obligations clear. Other agreements routinely include reciprocal confidentiality undertakings to protect the Trust's intellectual property rights and any personal data that may arise.

Subject access requests

Any request by an individual to have access to the personal data held by the Trust will be referred to the Trust Director. The request will be answered as soon as practicable and in any event within one month. It is the responsibility of the Trust Director to exercise his professional judgement or to seek external legal advice in any restriction of information disclosed if a request is received.

Dealing with a data breach

If there is a data breach it is the responsibility of the Project Manager and/or the Administrator identified in the data inventory to notify the "Data processor" as soon as possible. The issue will be investigated by the senior management team and rectified. Anyone affected by the data breach will be contacted and any mitigation required will be agreed and implemented.

Direct marketing

The Trust will not use personal data for fundraising purposes or soliciting support, except where there is express consent. The Trust will not use personal data for other direct marketing of goods or services.

Right to prevent use of data

As a matter of routine, the Trust Director will arrange that any person who does not wish to receive any communication from the Trust accede to such a request.

Other than to maintain an audit trail for the Trust's auditors or the Government's auditors where public grants are involved, or the data is processed in such a manner so as prevent any individual identification (e.g. market research data), the Trust Secretary will arrange for any other personal data the subject of a request to be deleted or provide an explanation in writing to the contrary.

Review of Policy

The Trust Director will review this Policy upon each renewal or registration change or more frequently if circumstances dictate or suggest otherwise. Any issues identified will be raised with the Trustees at the soonest opportunity.