

DATA PROTECTION POLICY

Policy statement

The Trust is committed to a policy of protecting the rights and privacy of Trustees, co-opted Board and sub-committee members, contracted personnel, volunteers, general public and any other individuals connected with the Trust, in accordance with the General Data Protection Regulation (GDPR). The policy applies to all Trustees, contracted workers and volunteers.

As a matter of good practice, any organisations and individual working directly with the Trust, who has access to personal information relating to Trustees, co-opted members, contractors, volunteers or service users will be expected to comply with this policy. Any Trustee, volunteer or contracted worker who deals with external organisations will be responsible for ensuring that they are aware of and agree to abide by this policy.

Legal Requirements

The General Data Protection Regulation (GDPR) has applied since 25 May 2018, when it superseded the UK Data Protection Act 1998 (DPA). Its purpose is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is not processed without their consent.

The Regulation requires the Trust to register the fact that it holds personal data and to acknowledge the right of 'subject access', i.e. volunteers, contracted staff, Trustees, co-opted members and service users have the right to see or have a copy of any data relating to themselves.

Managing Data Protection

The Trust will ensure that if its details are required to be registered with the Information Commissioner it will do so, by checking criteria in January each year.¹ Whether required to register or not, the Trust is still required to apply by the principles of the GDPR.

Purpose of data held by the Trust

Data may be held for the following purposes:

1. Recruiting and appointing contractors
2. Management of any contracted personnel
3. Contacting individuals who use or may be interested in the Trust's work or services
4. Managing, supporting and training volunteers
5. Realising the objectives of the Trust, as an unincorporated voluntary body
6. Accounts and records
7. Fundraising and contacting potential supporters
8. Review and evaluation of the Trust
9. Promotions, publicity and public relations
10. Information and database administration

In the case of 5 to 10, only anonymised summaries would be held and used.

¹ The Trust is exempt from registration as of August 2018 but eligibility criteria will be checked annually to ensure that this exemption still applies. <https://ico.org.uk/for-organisations/data-protection-fee/self-assessment>

Data Protection Principles

In GDPR terms the Trust is the 'data controller', and as such determines the purpose for which, and the manner in which, any personal data are, or are to be, processed. The Trust must ensure that any personal data it holds is:

1. Fairly and lawfully processed

The Trust will always state its intentions on processing the data and indicate whether, and to whom, we intend to give any personal data; also an indication of the duration the data will be kept.

2. Processed for limited and agreed purposes only

The Trust will not use data for purposes other than those agreed by data subjects (volunteers, members, paid or contracted workers, visitors, public and anyone else.) If the data held is requested by external organisations for any reason, this will only be passed with the agreement of the data subjects (as above). External organisations seeking access to personal data must state the purpose of processing, agree not to copy the data for further use and agree to abide by the GDPR and the Trust's Data Protection Policy, in writing if appropriate.

3. Adequate, relevant and not excessive

The Trust will regularly monitor the data held for its purposes, ensuring neither too much nor too little data is held in respect of the individuals about whom the data is held. If data given or obtained is excessive or unnecessary for the purposes itemised earlier in this policy, it will be deleted or destroyed.

4. Accurate, up-to-date and consented

The Trust will offer to provide everyone about whom personal information is held, with a copy of their data annually for information and updating where relevant. All amendments will be made promptly and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data the Trust holds is accurate and up-to-date. Completion of an appropriate form signed by the individual will be taken as an indication that their data is accurate and that the individual has consented to the Trust holding it. Individuals should notify the Trust of any changes, to enable personal records to be updated accordingly. The Trust is responsible for acting upon notification of changes to data, amending it where relevant.

5. Not kept longer than necessary

The Trust discourages the retention of data for longer than it is required. All personal data will be deleted or destroyed after two years of non membership or non-involvement has elapsed unless it is deemed appropriate to hold it for follow up purposes and maintaining contact. However paper copies will be destroyed and not held by the Trust.

6. Processed in accordance with the individual's rights

All individuals that the Trust holds data on have the right to:

1. The removal and correction of any inaccurate data about them.
2. Be informed about any request to access any data held about them by third parties.
3. Prevent the processing of their data for the purpose of direct marketing.
4. Compensation if they can show that they have been caused damage by any contravention of the Regulation.

7. Secure

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, damage or destruction of data. Specifically, anyone viewing or storing personal data on their computers should have a log in system to prevent unauthorised access. Passwords should be changed frequently. Paper copies of financial and personal records are to be kept in a secure place which can only be accessed by designated personnel.

8. Not transferred to countries outside the European Economic Area

Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual and unless the country has adequate protection for the individual. The Trust will take particular care to be aware of this when publishing information on the internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the European Economic Area.

Review

This policy will be reviewed every three years or sooner if there is a significant change in the operation or responsibilities of the Trust or if there is a significant change to the GDPR or other data protection legislation which could affect the Trust.