Daisie Rich Trust
Data Protection Policy

Last updated: 25th May 2018

Definitions:

Trust	means Daisie Rich Trust, a registered charity
GDPR	means the General Data Protection Regulation

1. Data protection principles

The Daisie Rich Trust is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2. General provisions

a. This policy applies to all personal data processed by the Trust.
b. The Trust will take responsibility ongoing compliance with this policy.
c. This policy will be reviewed at least annually.
d. The Trust will register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Trust will maintain a register of its systems.
b. This register will be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Trust will be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Trust must be done on one of the following lawful bases: consent; contract; legal obligation; vital interests; public task or legitimate interests.
b. The Trust will record the appropriate lawful basis in its register.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems will be in place to ensure such revocation is reflected accurately in the Trust's systems.

5. Data minimisation

a. The Trust will ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Trust will take reasonable steps to ensure that personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps will be taken to ensure that personal data is kept up to date.

7. Retention / removal

a. To ensure that personal data is kept for no longer than necessary, the Trust will have a retention policy for each area in which personal data is processed, and will review this process annually.
b. The retention policy will consider what data should / must be retained, for how long and why.

8. Security

a. The Trust will ensure that personal data is stored securely using modern software, that is kept up-to-date.
b. Access to personal data will be limited to personnel who need access and appropriate security will be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely in order that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions will be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data, the Trust will promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

END OF POLICY