Safeguarding and Welfare Requirements: Welfare	
Policy Name:	**Data Protection — GDPR Procedure**
Policy Creation Date:	**January 2019**
Last review:	**January 2022**
Next review:	**January 2023**
Owner:	**HR/Operations Director**
Related Documents:	**Data Breach Checklist - Appendix 23**

- **Designated Data Controllers and Data Protection Officers**

The Designated Data Controllers: The Office Manager; the Service Manager (Children) and the Service Manager (Adults) will deal with day-to-day matters. Any member of staff, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with one of the above-named persons.

- **Staff Responsibilities**

All employees are responsible for:

- checking that any information that they provide to the Charity in connection with their employment is accurate and up to date
- informing the Charity of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The Charity cannot be held responsible for any errors unless the employee has informed it of such changes.

- **Data Security**

All employees are responsible for ensuring that:

- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Employees should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

- **Disaster Recovery**

1. The Charity backs up data daily, with a full back up being taken on a Friday. Records of passes and failures are retained by the IT Service Provider.

2. Backups are kept on the NAS box in the workroom.
3. In case of failure of a full main backup a new one is done the following Friday.
4. Firewalls and virus checkers are kept up to date and running.
5. The Charity plans for how to deal with loss of electricity, external data links.
6. The IT Service Provider advises on loss of electricity, server failure, and network problems.

- **Subject Consent**

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, the Charity takes a "granular" approach i.e. it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the Charity ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following.

- Contract: if processing someone's personal data is necessary to fulfil the Charity's contractual obligations to them (e.g. to provide a quote).
- Legal obligation: if processing personal data is necessary to comply with a common law or statutory obligation.
- Vital interests: not one that will occur often as it refers to processing personal data to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent.
- Legitimate interests: the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Note that the GDPR provides for special protection for children's personal data and the Charity will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

- **Subject Access**

An employee may request details of personal information which the Charity holds about him or her under the GDPR. A small fee may be payable and will be based on the administrative cost of providing the information. If an employee would like a copy of the information held on him or her, they should write to the Operations Director. The requested information will be provided within one month. If there is any reason for delay, that will be communicated within the four-week time period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If an employee believes that any information held on him or her is incorrect or incomplete, then they should write to or email the Operations Director as soon as possible. The Charity will promptly correct any information found to be incorrect.