

Data Protection Policy

Last updated	05 March 2021
Definitions	
Charity	It's a Penalty, registered charity no. 1161848
GDPR	means the General Data Protection Regulation.
Responsible Person	Sarah de Carvalho CEO
Internal Register of System	Here we list all documents we have in place (systems) showing the charity's compliance with general provisions that are applicable e.g. Data protection policy, Terms & Condition, Procedures, Archive policy

1. Data protection principles

It's a Penalty is committed to processing data in accordance with its responsibilities under the GDPR provisions.

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

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those 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;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- kept in a form which permits identification of 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
- 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 data processed by the Charity on individuals and partners organisations.
- b. This policy is reviewed at least annually;
- c. The Charity is registered with the Information Commissioner's Office as an organisation that processes personal data;

- d. The Charity was established for not-for-profit making purposes and does not make a profit;
- e. We only process information necessary to establish or maintain membership or support from partner organisations;
- f. We only share the information with people and organisations necessary to carry out our activities and;
- g. We only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration.

3. Lawful, fair and transparent processing

- To ensure data processing remains lawful, fair and transparent, the Charity maintains a Register of Systems.
- Register of Systems mean a folder containing all the documents and policies and procedures created to ensure we are complying with the GDPR.
- The Register of Systems is reviewed at least annually. This means every document inside the registry is reviewed.
- Individuals and partners organisations have the right to access the data we hold on them and any such requests made to the charity shall be dealt with in a timely manner.
- Individuals and partners who wish to have their data deleted from the Charity's systems can do so any time via email request or by 'unsubscribing' from communications sent by the Charity.

4. Lawful purposes

- All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).

Therefore, the Charity determines that the lawful basis for its data processing is consent.

5. Lawful handling

- Everyone who works for the Charity has some responsibility for ensuring data is collected, stored and handled appropriately.
- The Charity shall make available to all individuals and partners how their data is handled.
- The only people able to access data covered by this policy are those who need it solely for their work with It's a Penalty and absolute confidentiality will be maintained and not used for any other purpose whatsoever in the course of their work with any other business.
- Evidence of opt-in consent, including a consent statement, shall be kept for each individual that the Charity wishes to retain data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent shall be clearly available and systems are in place to ensure such revocation is reflected accurately in the Charity's systems.
- The Charity shall ensure that personal data is relevant and limited to what is necessary in relation to the purposes for which they are processed.
- The Charity shall take reasonable steps to ensure personal data is accurate.
- To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving procedures policy.
- The archiving policy shall consider what data should/must be retained, for how long, and

why.

- Employment and consultant contracts will be retained for five years after the end of contract and those who enter into any form of contract with the Charity may request that their record/s be destroyed. Any electronic copies will be kept for similar periods. These Contracts only hold Name and address.

6. Offline data storage

- When data is stored on paper, it shall be kept in a secure place where unauthorised people cannot see it;
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason;
- Employees/Consultants/Trustees and volunteers will make sure paper and printouts are not left where unauthorised people could see them, like on a printer;
- Data printouts shall be shredded and disposed of securely when no longer needed.

7. Online data storage

It's a Penalty Employees, Consultants, Trustees and Volunteers comply with the appropriate data protection remit for online data storage

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data shall be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data shall only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data shall be sited in a secure location, away from general office space.
- Data shall be backed up frequently.
- All servers and computers containing data should be protected by approved security software and a firewall.

- **Data use**

It's a Penalty Employees, Consultants and Volunteers will comply with the appropriate data use remit for online data storage

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data shall not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Employees should not save copies of personal data to their own computers.

9. Data Security

- The Charity is committed to ensure that personal data remains stored securely using modern software that is kept-up-to-date.
- Access to personal data is strictly limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information.
- When personal data is deleted such data is irrecoverable.

10. Breach

- In the event of a breach of security leading to the accidental or unlawful alteration or unauthorised disclosure of, or access to, personal data, the Charity shall promptly contact the the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Charity will inform those individuals without undue delay.
- The Charity shall keep a record of any personal data breaches.

END OF POLICY