Policy is applicable to: This policy applies to staff, trustees and volunteers.

Consortium aims to fulfil its obligations under the General Data Protection Regulations (formerly under the Data Protection Act 1998). We also uphold principles held in the Human Rights Act and guidance from the Information Commissioners Office.

All personal data will be held in accordance with the principles and requirements of data protection and relevant legislation and procedures to ensure the fair processing of all data.

Responsible Officer

The responsible Officer for this policy is the Chief Executive Officer, currently Paul Roberts. This Officer is the official Data Protection Officer (DPO) for the organisation.

In their absence, the responsibility of this policy lies with the Chair of Trustees, currently Helen Belcher.

Data Protection Principles

The following principles guide our approach to Data Protection and fulfilling our requirements under the law:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. 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;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. 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
5. 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
6. 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 measure

General Provisions

This policy applies to all personal data processed by the Charity.

This policy shall be reviewed at least annually.

Where required, the charity will register with the Information Commissioner's Office as an organisation that processes personal data.

Lawful, Fair and Transparent Processing

In order to ensure data processing is lawful, fair and transparent, the Charity shall maintain a Data Control Register.

This Register shall be reviewed at least annually.

Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

Lawful Purposes

All data process by the charity must be done on one of the following lawful bases:

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests

The charity shall note the lawful basis in the Data Control Register.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

Data Minimisation

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

Key data processed by the Charity, and the timescale for retention are as follows:

1. Staff Information: for 7 years following end of employment
2. Applicants Information: For 6 months following successful recruitment
3. Board Information: for 5 years following end of Trusteeship
4. Member Information: During active membership, and for 6 months after
5. Survey Data: If identifiable, 1 year. If anonymised, can be archived for future use or further analysis
6. Event Webforms: 1 month following the event
7. Project webforms: 6 months following completion of the project
8. Contact Forms: deleted after request complete or actioned
9. Mailing Lists: only whilst active consent is given, renewed every 12 months
10. Staff Files: for 5 years following completion of piece of work, unless personal data which will be deleted immediately. All funding information will be kept indefinitely.

Security

The Charity shall ensure that personal data is stored securely using modern software that is kept up to date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

When personal data is deleted this should be done safely such that the data is irrecoverable.

Appropriate backup and disaster recovery solutions shall be in place.

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 Charity shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office.

Responsibilities

It is the responsibility of the responsible Officer to:

- Ensure this policy is kept up to date
- Ensure that all appropriate data capturing procedures are in place
- Ensure that data is stored securely
- Ensure requests for access to personal information are recorded

It is the responsibility of employees, trustees and volunteers to:

- Ensure they understand the policy
- Not disclose any personal information held on trustees, employees, volunteers, or individuals from Member organisations (this is also monitored through the Confidentiality Policy)
- Make a request to access any personal information

Procedures

Personnel Records

The names and post held of staff within the Charity are considered to be in the public domain and may be made freely available in any format.

The names, organisation and role held of Trustees within the Charity are considered to be in the public domain and may be made freely available in any format.

Addresses, phone numbers, personal emails addresses shall only be made to staff, trustees or volunteers only for the purpose of making contact in furtherance of the Charity's governance. Consent must be obtained for sharing of personal information, unless in an emergency situation.

Member Database

Data on Members, and individuals within that Member organisation, shall be confined to contact details and information directly relevant to the reason for their inclusion in the Charity's database or CRM. Data considered non-personal (i.e. financial information and areas of operation) may be held securely for the furtherance of the Charity's operations.

Business Use by Personnel

Staff, trustees and volunteers using the Charity's IT equipment should be aware that senior staff and appropriate trustees can access this equipment in the furtherance of the Charity's operations or governance requirements. This extends to email accounts and files kept on local drives.

All users of the Charity's equipment are requested to minimise personal contact through IT equipment (e.g. emails) and personal information should be marked as "personal". All users are also advised that anyone sending personal information should mark correspondence as "personal".

If a member of staff, trustees or volunteers are absent for any period of time access to (e.g.) email inboxes for the purposes of responding to urgent correspondence or adding an out of office advisory note shall be granted by a senior member of staff.

In line with the Charity's disciplinary and grievance procedures, access to business equipment may be necessary to support any investigation. Where this is applicable, the access shall be limited to business related data unless otherwise agreed in advance by the member of staff, trustee or volunteer.

In line with our Intellectual Property procedures, all information kept within the Charity's systems falls within the remit of this Policy.

Cloud Based Systems

The Charity uses cloud-based systems for the day to day operations of the organisation. All data stored on cloud-based servers are the responsibility of the Charity and systems put in place to ensure data security.

Emails, calendars and contacts are all stored on the Charity's cloud-based system and shall be retained as per our data minimisation process as detailed in this Policy.

Recruitment

If you are applying for a role with us (whether as a member of staff, a volunteer or trustee), we collect information from you in the curriculum vitae (including any drafts) and any other documents that you send us, and from what you tell us during interview. We may also look at publicly available sources of information such as LinkedIn and any online, public profile with your existing employer. All such information is stored and used in accordance with this policy, including limitations on data retention

The right to be forgotten

Under GDPR rules, the right to be forgotten enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The Charity will fully comply with any requests from individuals under their right to be forgotten, unless this request contravenes the Charity's legal responsibility to retain relevant data.