DATA USE, RETENTION AND DISPOSAL POLICY

1. Introduction

   This policy sets out the obligations of the Organisation regarding personal data collected, held, and processed by the Organisation in accordance with the General Data Protection Regulation ("GDPR").

   It also sets out the type(s) of personal data held by the Organisation, the period for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

   This policy should be read in conjunction with the Employee Privacy Notice.

2. Scope of Personnel

   This policy applies to all personnel involved with the Organisation such as volunteers, subsidiaries, consultants and associates. An associate includes any person working as a subcontractor; as a joint venture partner or agent. For the purposes of this policy, all these entities shall be collectively referred to as "volunteers" or "you".

   These procedures do not form part of your contract and are therefore non-contractual except where it is expressly stated or where statute is in place to imply otherwise.

3. What is personal data?

   The GDPR defines "personal data" as any information relating to an identified or identifiable natural person.

4. How long can personal data be retained?

   Under the GDPR, personal data can be kept in a manner which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.. The Privacy Notice has full details about the different types of data that can be retained and the purpose for which they are held.

   In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the

implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

5. Right to be forgotten

   GDPR includes the right to erasure or "the right to be forgotten". Personnel covered by this policy have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

   the personal data is no longer required for the purpose for which it was originally collected or processed
   when the data subject withdraws their consent
   when an individual objects to the processing of their personal data and the Organisation has no overriding legitimate interest
   when the personal data is processed unlawfully (i.e. in breach of the GDPR)
   when the personal data has to be erased to comply with a legal obligation.

6. Scope of Data Held

   This policy applies to all personal data held by the Organisation and by any third-party data processors processing personal data on behalf of the Organisation.

7. How is personal data stored?

   Personal data held by the Organisation is stored using Cloud technology. The process is managed by the Organisation's IT provider. Data is held using the following methods:

   laptop computers and other mobile devices provided by the Organisation to Directors, Line Managers and Administration staff
   laptop computers and other mobile devices provided by clients to Directors, Line Managers and Administration staff
   computers and mobile devices owned by Directors, Line Managers and Administration staff
   physical records stored on Organisation property
   physical records stored at the homes of Directors, Line Managers and Administration staff, who are working from home.

8. Data subject (Volunteers) rights and data integrity

All personal data held by the Organisation about you is kept in accordance with the requirements of the GDPR and the Organisation's Privacy Notice.

The Organisation Privacy Notice provides you with information about your rights, of what personal data the Organisation holds about you, how that personal data is stored and for how long it will be retrained.

You have control over the personal data that is held by the Organisation about you, including the right to have incorrect data rectified, the right to request that your personal data be deleted or otherwise disposed of (notwithstanding the retention periods as set out in the Privacy Notice)

9. Technical and Organisational Data Security Measures

The Organisation have in place several technical measures to protect the security of personal data:

- personal data may only be transmitted over secure networks. Email is not considered to be secure. If you are required to transmit personal data via email, it should be encrypted or password protected prior to sending.
- personal data may not be transmitted over a wireless network if there is a reasonable wired alternative
- where personal data is to be transferred in hardcopy form, it will be passed directly to the recipient or sent using a reputable delivery service
- no personal data may be shared informally, and if access is required to any personal data, such access should be formally requested via the Organisation Secretary
- hard copies of personal data, along with any electronic copies stored on physical media should be stored securely
- personal data may only be transferred to an employee, agent, contractor, or other third party if the transference complies with the Organisation’s Privacy Policy
- personal data must be handled with care at all times and should not be left unattended or on view
- computers used to view personal data must always be locked before being left unattended
- no personal data should be stored on any mobile device whether such device belongs to the Organisation or otherwise without the formal written approval of a Director
- no personal data should be transferred to any device personally belonging to an employee, and personal data may only be transferred to devices

belonging to agents, contractors, or other parties working on behalf of the Organisation where the party in question has agreed to comply fully with this policy and with the Organisation's Privacy Notice

- all personal data stored electronically should be backed up and the backups encrypted
- all electronic copies of personal data should be stored securely using passwords and encryption
- all passwords used to protect personal data should be changed regularly and must be secure
- under no circumstances should any passwords be written down outside of one's personal premises
- passwords should never be shared. If a password is forgotten, it must be reset using the correct protocol
- all software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available
- no software may be installed on any Organisation-owned computer or device without approval
- where personal data held by the Organisation is used for marketing purposes, it shall be the responsibility of the client manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS
- all personnel and other parties working on behalf of the Organisation shall be made fully aware of both their individual responsibilities and the Organisation's responsibilities under the GDPR and under the Organisation's Privacy Policy
- only personnel and other parties working on behalf of the Organisation that need access to, and use of, personal data to perform their work, shall have access to personal data held by the Organisation
- all personnel and other parties working on behalf of the Organisation handling personal data will be appropriately trained to do so
- all personnel and other parties working on behalf of the Organisation handling personal data should exercise care and caution when discussing any work relating to personal data at all times
- methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- all personnel and other parties working on behalf of the Organisation handling personal data belonging to volunteers or others will be bound by contract to comply with the GDPR, this Policy and the Organisation's Privacy Policy
- all agents, contractors, or other parties working on behalf of the Organisation handling personal data must ensure that others working with personal data

belonging to Organisation's volunteers or others will be bound by contract to comply with GDPR, this Policy and the Organisation's Privacy Policy

- where any agent, contractor or other party working on behalf of the Organisation handling personal data fails in their obligations under the relevant Organisation policies, that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

10. Data Disposal

Upon the expiry of the data retention period of 7 years as set out below in this policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- personal data and sensitive personal data stored electronically (including any and all backups) shall be deleted
- hard copies of personal data or sensitive personal data shall be shredded using a secure shredding service. This can be organised via the Organisation Secretary

11. Data Retention

The Organisation shall not retain any personal data or sensitive personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

- Personal data about employment will be held for 7 years post-employment termination.
- Personal data contained in a Service Agreement entered into by the Organisation and a third party supplier shall be held for 7 years from the date that the Service Agreement terminated.

Roles and Responsibilities

The Organisation's Data Protection Officer is the Company Secretary.

The Data Protection Officer shall be responsible for overseeing the implementation of this policy and for monitoring its compliance and the compliance of the Organisation's other data protection-related policies (including, but not limited to, its Privacy Policy). The Data Protection Officer is also

responsible for ensuring compliance with current and future UK data protection legislation.

Line Managers are responsible for ensuring the compliance of their staff and should take any concerns to the Data Protection Officer.

Any questions regarding this policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.