DATA PROTECTION POLICY

Definitions:

GDPR	means the General Data Protection Regulation.
Responsible Person	means Michelle Bailey, Managing Director
Register of Systems	means a register of all systems or contexts in which personal data is processed by EASE.

EASE 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 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;
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 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 EASE.
b. The Responsible Person shall take responsibility for EASE's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. EASE shall 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, EASE shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.

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

4. Lawful purposes

a. All data processed by EASE 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).
b. EASE shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall 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 should be clearly available and systems should be in place to ensure such revocation is reflected accurately in EASE's systems.

5. Data minimisation

a. EASE shall 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. EASE shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date7. Archiving / removal
a. To ensure that personal data is kept for no longer than necessary, EASE shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. EASE shall ensure that personal data is stored securely using modern software that is kept-up-to-date or within locked files.
b. 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.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall 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, EASE shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Obligations on staff working at the settings

The obligations outlined in this policy apply to all those who have access to personal data held by the organisation.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or is deliberately acts outside of their recognised responsibilities may be subject to disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution. All individuals permitted to access personal data in line with their work duties must comply with this policy and agree to undertake any relevant training that may be appropriate to the job/position being undertaken.

Confidentiality and Security

- Manual files (paper records) – access is restricted solely to the relevant staff and stored in secure locations (e.g. lockable cabinets) to prevent unauthorised access.
- Computer systems and files are firewall and password protected.
- Those who use equipment in EASE settings/sessions will have access only to the data that is both necessary for the work they are doing and held for the purpose of carrying out that work. Data users must comply with EASE's Security measures.
- Personal data will only be disclosed to legitimate recipients. This varies according to the nature of the data and the purpose for which it is intended. Permission for data disclosure to anyone who is not a member of staff at EASE may only be given by the Managing Director, or it pertains to the records of Service Providers at the setting by the Managing Director
- Sensitive Personal Data e.g. child protection issues, staff personal details may be restricted even from the subject under certain circumstances, e.g. if the release of data may result in harm. If this is the case the Manager will be consulted for advice.

Service Providers

All Service Providers are responsible for ensuring that they and their staff provide induction and job-specific training to their staff and volunteers regarding this policy area. Service Providers are also responsible for the monitoring and adherence to the Data Protection Policy.

Policy Implementation:

- The Managing Director/Trustees are responsible for the implementation of this policy and conducting regular reviews.
- All staff are made aware of this policy as part of their induction, reviews, and training.
- All clients are made aware of this policy and are encouraged to follow the guidelines – privacy statement available on the EASE noticeboard in the setting
- Partner agencies are made aware of this policy and sign an agreement to support its implementation.

Policy Review

This Policy will be reviewed annually or earlier if an update is deemed necessary due to legislation or best practice

This policy was reviewed and approved by the Trustees on	6.7.22
Next policy review date	6.7.24