Version: 1
Status: Approved
Next Review: 25th May 2019

Data Protection Policy Statement

1. Policy Objectives

1.1 By publishing this policy statement EnhanceAble aims to ensure compliance with key policy objectives. The key policy objectives set out what is to be achieved by implementing the policy.

1.2 All staff are responsible for ensuring compliance with key Policy objectives.

No	Data Protection Key Objective
1	To ensure compliance with the General Data Protection Regulation (GDPR)
2	This policy has been approved by the EnhanceAble management team and has the support of the EnhanceAble trustees who are ultimately responsible for compliance with Data Protection legislation.
3	The management team has responsibility for maintaining, publicising and implementing this policy.
4	The General Data Protection Regulations require that the data subject is provided access to their data within 30 days of their request being validated by EnhanceAble. EnhanceAble will endeavor to provide the data requested well before the 30 day limit.
5	All staff will be provided with data protection training and will be expected to comply with data protection legislation and adhere to EnhanceAbles Data Protection policies and procedures.
6	EnhanceAble will appoint a Senior Information Risk Owner from within its existing trustees and a Data Controller form within its existing staff team. These individuals alongside the CEO will take primary responsibility for the management of personal data.

2. Policy Statement

EnhanceAble is required to store personal data about its staff and services users in order to legitimately carry out its business. In the light of this It is the EnhanceAble Policy that;

- Personal data are processed fairly and legally
- Personal data are only obtained for specified and lawful purposes

- Personal data are adequate, relevant and are not excessive to the purposes for which they are processed.
- Personal data are kept accurate and up to date.
- Personal data are not kept for longer than is necessary.
- Personal data are processed in accordance with the rights of the data subjects
- Personal data are protected from unauthorized and unlawful processing and against accidental loss or destruction or damage by appropriate technical and organizational controls.

3. Subject Access

3.1 The Data Subject can be anyone about who EnhanceAble retains personal data. Most commonly this will be service users, staff and other stakeholders. From time to time any of these stakeholders might request access to that personal data. This is called a Subject Access request.

3.2 The CEO, Data Controller and Senior must be informed of all subject access requests.

3.3 Personal data will only be disclosed to the data subject (or his/ her representative) when;

- The subject access request is made in writing or audio recorded in cases where people have difficulties around writing.
- The authenticity of the individual making the request has been confirmed.
- The data subject has given their documented consent for the representative to receive the data requested (where the request is made by a representative of the data subject)
- The appropriate fee has been paid where required (Max £10). Note: this fee will not apply to service users, relatives of service users or staff.

3.4 The response time detailed in section 1 does not commence until all conditions identified in section 3.3 have been satisfied.

3.5 Requests for service user's personal data will be coordinated by the relevant manager. Usually the manager of that service.

3.6 Requests for staff personal data will normally be coordinated by the HR Manager.

3.7 A written record of all requests will be maintained for all Subject Access requests.

3.8 All data will be reviewed and any personal data relating to 3rd parties will either be removed, anonymised or consent for its disclosure obtained from the 3rd party.

3.9 When a data subject is provided with direct access to a manual file a member of EnhanceAble staff must be present at all times.

3.10 Responses to subject access requests must include personal data processed by relevant data processors.

4. Personal Data Breaches

4.1 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

4.2 EnhanceAble has an obligation to report certain types of personal data breach to the relevant supervisory authority. EnhanceAble will do this within 72 hours of becoming aware of the breach, where feasible.

4.3 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, EnhanceAble will also inform those individuals without undue delay.

4.4 EnhanceAble will retain a record of any personal data breaches, regardless of whether we are required to notify.

5. Data Audits

EnhanceAble will carry out an annual data audit at each of its services in order to ensure that personal data is stored and deleted as appropriate and in accordance with relevant data protection legislation.

5.1 The audit will be the responsibility of the manager of that service with support from other relevant managers at EnhanceAble.

6. Associated Policy and Procedure

This Policy statement should be read in conjunction with the following procedures;

- Data Protection Procedure.
- Confidentiality Procedure.
- Data Protection-staff guidelines.

7. Diversity and Inclusion

7.1 Enhanceable treats all its service users, staff and other stakeholders with fairness & respect. We recognize that we have an ethical and legal duty to advance equality of opportunity and prevent discrimination on the grounds of age, sex & sexual orientation disability, race, religion or belief gender assignment, pregnancy and maternity, marriage and civil partnership.

7.2 This document and any related literature may be translated or interpreted or provided in accessible formats as necessary.

7.3 Diversity and inclusion training is mandatory for all EnhanceAble staff.

8. Governance, Monitoring and Review.

This policy will be reviewed annually by the CEO. EnhanceAble's trustees will be made aware of any changes to this policy.

Version No	1
Status	Approved
Effective date	25th May 2018
Signed off by	N/A
Author	Julie Hagarty / Hannah Bryce.
Review Date	25th May 2019.

Information Procedures

1. Information that we hold.

In order to safeguard individuals, our employees and our charity, EnhanceAble are required to keep detailed information about people. The information we keep may consist of any or all of the following:

Person Type	Data Type	Data Form
Service User	Support plans	Paper & Electronic
Service User	Risk Assessments	Paper & Electronic
Service User	Medication profile	Paper & Electronic
Service User	Photo consent	Paper & Electronic
Service User	Meeting notes	Paper & Electronic
Service User	Referral Information	Paper & Electronic
Service User	Correspondence	Paper & Electronic
Relatives	Contact details	Paper & Electronic
Staff	Bank details	Paper & Electronic
Staff	National Insurance number	Paper & Electronic
Staff	NOK information	Paper & Electronic
Staff	DBS information	Paper & Electronic
Staff	Application CV	Paper & Electronic
Staff	Car insurance	Paper & Electronic
Staff	performance data	Paper & Electronic
Stakeholder	professional contact details	Paper & Electronic
Stakeholder	Bank details	Paper & Electronic
Relative	Bank details	Paper & Electronic

2. Record Keeping & Storage (Service Users)

1.1 EnhanceAble will keep clear and accurate records in plain English giving details of our work with service users.

1.2 EnhanceAble will keep a separate file for each service user's information. This file will be kept in a locked cabinet in the EnhanceAble Living office.

1.3 For EnhanceAble Living service users, individual activity and support records will be kept within the service users home for one month and then transferred to the person's file in the EnhanceAble Living office. If people do not want their files kept at home during this interim period, they can choose for them to be kept in the EnhanceAble Living offices.

1.4 All EnhanceAble Space records will be kept in the home. They will only be transferred for secure archiving in our head office or another secure location.

1.5 All records will be kept in clear, legible writing.

1.6 All records will be factual and non-judgemental. Staff will not theorise in people's files

1.7 All files will be accessible only to relevant staff. Staff will not share details with other agencies or individuals without the permission of the service user.

1.8 EnhanceAble staff will only break confidentiality when they believe that person, or another person to be at risk of serious harm.

1.9 Any records, letters etc relating to a service user that are kept electronically will be password protected.

1.10 In addition to service user's discreet files, the following records will be maintained:

- An accident book
- An Incident file
- A complaints file
- A file of reports of suspected abuse

3. Record Keeping & Storage (Staff)

EnhanceAble keeps records on all staff and volunteers. The Manager of the individual service retains all information, except payroll data which is held by the Finance Officer.

All personal details is stored on a secure server and / or in a lockable facility accessible only to the relevant managers.

4. Access to Information.

The people who use our services their relatives or our staff may, from time to time make a request to see the personal data relating to them.

The General Data Protection Regulations calls this a Subject Access Request.

When this happens The CEO, Data Controller and Senior Information Risk Owner must be informed of all subject access requests as soon as is practically possible.

Personal data will only be disclosed to the data subject (or his/ her representative) when;

- The subject access request is made in writing or audio recorded in cases where people have difficulties around writing.
- The authenticity of the individual making the request has been confirmed.
- The data subject has given their documented consent for the representative to receive the data requested (where the request is made by a representative of the data subject)
- The appropriate fee has been paid where required (Max £10). Note: this fee will not apply to service users, relatives of service users or staff.

EnhanceAble will ensure that access is given within the 30 day limit and will endeavor to give access more rapidly than this.

Requests for service user's personal data will be coordinated by the relevant manager. This will usually be the manager of that service. Access to hard documentation will be supervised by an EnhanceAble employee.

Requests for staff personal data will normally be coordinated by the HR Manager.

5. Archiving and deleting Information

EnhanceAble will retain data for the following timescales;

Committee Minutes	10 years
Employment Folders	From 2000 onwards
Service user records	5 years post death of service user
Other documents	7 years.

Hard copy documents containing personal data will be destroyed by a specialist waste management company.

6. Data Breaches

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

EnhanceAble has an obligation to report certain types of personal data breach to the relevant supervisory authority. EnhanceAble will do this within 72 hours of becoming aware of the breach, where feasible.

The Data Controller / CEO/ Senior Information Risk Owner will have responsibility for deciding if a breach is reportable to the supervisory authority. The Data Controller/CEO will have responsibility for informing the the Supervisory Authority when a breach has taken place.

Any data breach should be reported to the Data Controller, Senior Information Risk Owner as soon as is practically possible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, EnhanceAble will also inform those individuals without undue delay. The Data Controller / CEO will be responsible for making this decision.

EnhanceAble will retain a record of any personal data breaches, regardless of whether the organisation is required to notify supervisory authority. The Data Controller will retain a register of breaches for this purpose.

7. Sharing Information.

EnhanceAble will always attempt to gain consent from its staff, service users and stakeholders prior to sharing personal data with 3rd parties.

Service users or their representatives are asked to complete consent to share document when accessing any EnhanceAble service. This document sets forth exactly what personal data the service is planning to keep and enables service users or their representatives to select which agencies EnhanceAble is able to share this data.

There are some circumstances where EnhanceAble may need tor supply information to a 3rd party without explicit consent. These cicumstances are set forth in some detail in Enhanceable's Confidentiality Policy.

Staff are asked to complete a similar form to confirm awareness of the personal data EnhanceAble retains in order to provide employment and meet regulatory requirements.

8. Data Audits

EnhanceAble will carry out an annual data audit at each of its services in order to ensure that personal data is stored and deleted as appropriate and in accordance with relevant data protection legislation.

The audit will be the responsibility of the manager of that service with support from other relevant managers at EnhanceAble.

A pro forma has been produced to enable the auditing process.