ENABLE

The Voluntary and Community Sector Learning and Skills Consortium

Data Protection Policy

2020/21

Change History

First Published:	21/07/2010	**Originally Created by:**	Data Officer
Person Responsible for Policy:	Enable CEO		

Date of Review	**Reviewed by**	**Policy changes**	**Approved by**	**Date of next review**
16 Feb 2018	Standards Officer	Changes to job titles to reflect new organisational restructure. Small changes to wording and referencing	Operations Manager	23 July 2018
13/09/2018	CEO	References to GDPR	Board of Trustees	10/09/2019
10/09/2019	SMT	No changes	Board of Trustees	10/02/2020
21/04/2020	SMT	No changes	CEO	21/04/2021
06/10/2020	BDM	Covid-19	SMT	21/04/2021

Strategic Commitment

Enable is the Data Controller under the Data Protection Act 1998 and the General Data Protection Regulation, which means that it determines what purposes the personal information that is held will be used for. It is also responsible for notifying the Information Commissioner's Office (ICO - which is an independent authority in the UK that promotes openness of official information and protection of private information) of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Enable needs to collect and use certain types of information about the Data Subjects (Any living individuals who are the subject of personal data held by an organisation) who come into contact with it in order to carry on our work. This personal information must be collected and dealt with in accordance Enable standards-– whether on paper, in a computer, or recorded on other material.

Purpose

The purpose of this policy is to allow Enable to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect Enable's funders, staff and other individuals;
- protect the organisation from the consequences of a breach of its responsibilities

Policy

This policy applies to:

- the head office of Enable
- its regional offices
- all parties operating on behalf of Enable

It applies to paid staff and volunteers.

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

Enable will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

Enable recognises that its first priority under GDPR and Data Protection Act is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands
- holding good quality information

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Enable will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Enable has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately).
- Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed.
- Failure to offer choice about data use when appropriate.
- Breach of security by allowing unauthorised access.
- Failure to establish efficient systems of managing changes to staff, leading to personal data being not up to date.
- Harm to individuals if personal data is not up to date.
- Insufficient clarity about the way workers' or volunteers' personal data is being used e.g. given out to general public.
- Failure to offer choices about use of contact details for staff and volunteers.

Implementation

Responsibilities

The Enable Board recognises its overall responsibility for ensuring that Enable complies with its legal obligations.

The Data Protection Officer (the person within an organisation responsible for the compliance with the Data Protection Act) is the CEO, with the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification of incidences, events and weaknesses to relevant organisations
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors. Data processors are defined in the Act as any person (other than an employee of the data controller) who processes personal data on behalf of the data controller.

ICT Support Manager is responsible for electronic security.

The Communication Officer is responsible for approving Data Protection statements on documents requiring personal details to be completed, such as questionnaires.

Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

Each delivery partner is responsible for their compliance with their Data Protection policy.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under Enable's disciplinary procedures.

Confidentiality

Confidentiality applies to a much wider range of information than that covered under Data Protection and GDPR, and therefore Enable has a separate Classified Data Policy.

Enable has a privacy statement for Data Subjects, setting out how their information will be used. This will be available on request, and a version of this statement.

Staff, contractors and volunteers will be required to sign the Information Security Policy Agreement indicating that they have been made aware of and understand their confidentiality responsibilities.

Where anyone within Enable feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. All such disclosures will be documented.

Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Enable has identified the following risks:

- Information passing between the head office and providers could go astray or be misdirected.
- Staff or volunteers with access to personal information could misuse it.
- Staff and Volunteers could continue to be sent information after they have stopped working for Enable, if their records are not updated promptly.
- Staff may be tricked into giving away information, either about funders or colleagues, especially over the phone, through “social engineering” - is the act of manipulating people into performing actions or divulging confidential information.

Access to information on the main computer system is controlled by function.

Data Recording and storage

Enable will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems are designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual is held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.

Enable will retain data on the following groups in line with the retention periods specified by the Prime Contractor / Funding Body:

- Learners, employees or other users of Enables services.
- Volunteers
- Staff

Archived paper records of Learners are stored securely in the Basement.

Subject Access

The Data Protection Act 1998 and GDPR gives individuals (data subjects) a number of rights including the right to access personal data that an organisation holds about them. This right of access extends to all information held on an individual and includes personnel files, student record files, data-bases, interview notes and emails referring to the individual. If an individual makes a request to view their information, it is known as a “Subject Access Request”. Any subject access requests will be handled by the Data Protection Officer.

Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer immediately to allow a response to be made within the 40 working days stipulated by the Act.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity must be verified before handing over any information.

Enable will charge £10 for a subject access request, which will be made clear to the Data Subject when they make a request.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Transparency

Enable is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed;
- what types of disclosure are likely;
- how to exercise their rights in relation to the data

Data Subjects will generally be informed in the following ways:

- Staff & Volunteers: in the staff handbook
- Learners/Employees, or others accessing Enable services: in the welcome/induction pack

Standard privacy statements will be provided to staff at head office and to branches for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

Consent

Consent will normally not be sought for most processing of information about staff, with the following exceptions:

- Staff details will only be disclosed for purposes unrelated to their work for Enable (e.g. financial references) with their consent.
- Staff will be given the choice over their personal mobile phone being made public.

Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about learner/employees will only be made public with their consent. (This includes photographs.) They will complete the standard release form for photographs.

'Sensitive' data about members and funders (including health information) will be held only with the knowledge and consent of the individual.

Direct Marketing

Enable will treat the following unsolicited direct communication with individuals as marketing:

- promoting any Enable services;
- promoting provider events;
- promoting sponsored events and other fundraising exercises;
- marketing the products of Enable;
- marketing on behalf of any other external company or voluntary organisation.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out in the privacy statement. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Enable marketing.

Enable has the policy of sharing lists (or carrying out joint or reciprocal mailings) only on an occasional and tightly controlled basis. Details will only be used for any of these purposes where the Data Subject has been informed of this possibility, along with an option to opt out, and has not exercised this option.

Enable will only carry out telephone marketing when consent has been given in advance, or the number being called has been checked against the Telephone Preference Service (a free service which is the official central opt out register on which you can record your preference not to receive unsolicited sales or marketing calls).

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Staff Training and Acceptance of Responsibility

Information for staff and volunteers is contained in the staff handbook.

All staff with access to any kind of personal data will have their responsibilities outlined during their induction procedures.

Data Protection will be included in the training for any volunteers.

Enable will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

COVID-19

Information collected and/or disclosure of cases:
As part of the obligation to ensure the health and safety of all employees, learners, adults, children, vulnerable people, visitors and contractors to our premises, Enable may (subject to requirements of applicable law) inform personnel and third-parties about COVID-19 cases. The disclosure of such information will be limited as much as possible. If it is necessary to disclose the name of the individual who has contracted COVID-19 (and this is otherwise permitted by applicable law), appropriate protective steps will be implemented and the individual who has contracted the virus, will be informed first of the intended disclosure.

Responding to individual rights requests:
Enable's efforts and attention may be focused on tackling the implications of the coronavirus outbreak, but care will be taken to avoid failure to meet deadlines associated with responding to individual rights requests. If Enable is concerned that it may not be able to meet such deadlines, this will be communicated to the relevant individuals as soon as possible

Law requirements and guidelines, including data security:
In light of the Coronavirus, it is particularly important that we, Enable, maintain a close watch on personal data and ensure that it is adequately safeguarded. The more sensitive the data that is being processed, the more robust the applicable security measures will be to protect such data. Additionally, Enable will ensure that they continue to meet the deadlines for notifying data protection regulators (and individuals, as necessary) of personal data breaches that trigger the notification requirement.

When collecting individual's personal information, including people's COVID-19 symptoms or any related test results, Enable will only collect the information needed to implement measures appropriately and effectively.

Any personal data Enable hold will be kept securely and only held for as long as is necessary.

As with any data collection, Enable will inform individuals about their rights in relation to their personal data, such as the right of access or rectification. Employees will also have the option to exercise these rights if they wish to do so, and to discuss any concerns they may have.

Enable will adopt a fair approach to handling individual's data. It will be transparent in its purpose and compliant with data protection law.

Privacy notice:
This addition to Enable's Data Protection Policy is in line with government guidance, in relation to the Coronavirus and the NHS COVID-19 test and trace.

We only collect information about you when you scan our QR code through the NHS COVID-19 test and trace, or if this is not able to be done, then through asking for personal details to ensure your safety whilst with us. This information is only collected to help us contact you should you have been near or in contact with someone who has a positive Coronavirus test result.

We will always tell you when we are collecting this information.

Information that we may ask you for:
Name
Email address
Contact telephone number

Data sharing - Keeping your personal data secure:
We endeavour to keep your personal data secure. However, there may be times when we need to pass on your information, but only where we are legally obliged to do so. We will keep the details to an absolute minimum, but we will tell you:

how we use your information
who we share your information with
how we keep your data secure
about your rights to see or change information held about you

We will not share your personal information with anyone else without your permission for any other reason.

This amendment only applies to this policy and conjunction with the Coronavirus pandemic and does not cover our other policies. It is important to note that this document provides tips and guidance only. It is intended to support and draw out areas of risk and complies with legislation.

Third-party data sharing:
It may be necessary for Enable to share new Coronavirus personal data with third parties. Enable will ensure care is taken when doing so, and where appropriate, data processing agreements will be compliant and in accordance with the requirements of the GDPR laws.

Policy Review:
The policy should be reviewed every year by the Data Protection Officer and the Board of Trustees.

Signed:_____

Position:_____

Date:_____