ENABLE
The Voluntary and Community Sector Learning and Skills Consortium

Information Exchange Policy

Change History

First Published:	20/05/2011	**Originally Created by:**	IS Group
Person Responsible for Policy:	Enable CEO		

Date of Review	**Reviewed by**	**Policy changes**	**Approved by**	**Date of next review**
19 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	Standards Officer	No Changes	CEO	17/09/2019
21/04/2020	SMT	No Changes	CEO	21/04/2021
06/10/2020	BDM	Covid-19	SMT	21/04/2021

Strategic Commitment

Enable needs to collect and use certain types of information about Data Subjects with whom we come into contact in the course of our work. This personal information must be collected and dealt with appropriately; including ensuring it is kept secure when stored at the Enable premises and when it is exchanged with other organisations.

Purpose

The purpose of this policy is to ensure the confidentiality, integrity and accessibility of information in the course of exchanging it with delivery partners, funding bodies and other agencies as required. Its purpose is also to ensure checks are undertaken on unknown individuals requesting personal data.

Policy

This policy applies to:
- All Enable Staff
- All Freelance Staff
- All Delivery Partners operating on behalf of Enable

It applies to paid staff and volunteers.

1. Information initiated by Enable

All Enable staff and volunteers must have read and apply the requirements of all associated polices when handling and exchanging information.

Delivery partners who exchange information with Enable must have their own policies and procedures to ensure the secure exchange of information. Delivery partners should have information classification guidelines and procedures in place for document handling and labelling. It is the role of Enable to ensure these are fit for purpose.

Enable will work with funding bodies to ensure the security of information exchanged via batch uploading and online MIS services; this includes ensuring the security of passwords and secure access fobs/tokens where applicable.

Enable will monitor the effectiveness of our information exchange practices and take remedial action where required in line with the requirements of all associated policies.

The method used to exchange information is dependent on the classification of the information. The Classification and Protective Marking Policy details the action to be taken in each case.

For the data classifications, Restricted and Confidential, electronic data must be encrypted for exchange using PGP Desktop. This is located on the MIS Officer's computer. When submitting data to the Skills Funding Agency by e-mail, the data must appear in a password protect Excel/Word Document attached to the email. The password should be sent to the Agency under cover of a separate e-mail.

When sending any Fax or E-mail then the following disclaimers must be included.

Fax Disclaimer – The following disclaimer must appear on ALL Faxes

The contents of this fax are confidential and privileged. If the reader is not the person named above, notice is hereby given that any disclosure, copying, distribution or dissemination of the contents is strictly forbidden. If you have received this in error please notify me by telephoning immediately and return the fax by post to the above address. (Postage will be reimbursed.)

E-mail Disclaimer – The following disclaimer must appear on ALL emails

This email and any attachments are only intended for the original recipient. They may contain confidential information. If you have received this email by mistake, please notify the sender now and delete all paper and electronic copies. The contents of this email may contain personal views. These views may not be the views of Enable, unless clearly stated. The contents of this email do not constitute a contract. Enable will not accept liability for financial or other loss or damage to property that recipients may suffer as a result of this email.

2. Information and data requested by other parties

The recipients of any request by e-mail or telephone must ensure the data request is a valid one and that the requester can be traced.

Reponses to requests for data should be in accordance with the Classification and Protective Marking Policy and the procedures for dealing with sensitive information requests.

Where requests are made in person by and unknown individual, the requesters identification must be sought and verified. If it cannot be verified, then the request should be turned down.

COVID-19

This addition to Enable's Information exchange 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, 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.

Related Documents and Location
Document Handling and Labelling Procedure
Information Classification & Protective Marking Policy
Security Procedure for Sensitive Information Requests
Information Security Policy

Signed:_____

Position:_____

Date:_____