ENABLE

The Voluntary and Community Sector
Learning and Skills Consortium

Information Security Policy

Original Date: **2/9/11** Review Date: 23 July 2018

Change History

First Published:	02/09/2011	**Originally Created by:**	IS Group
Person Responsible for Policy:	Enable CEO		

Date of Review	**Reviewed by**	**Policy changes**	**Approved by**	**Date of next review**
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
21/04/2020	CEO	No Changes	CEO	21/04/2021

Strategic Commitment

The security and protection of information is fundamental to the effective and efficient operations of ENABLE and the maintenance of confidentiality.

Security is everyone's responsibility and all personnel working in the organisation must comply with this policy.

Scope of Policy

To meet legal requirements and satisfy obligations to its funders, ENABLE must use security measures to safeguard its information resources.

The ENABLE Information Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The policy of ENABLE is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised industry standard best practices that will mitigate against risk.

The policy applies to all information whether spoken, written, printed or computer based which is owned, held in custody of or used by ENABLE.

The policy also applies to all resources used in creating, processing, transmitting, storing using or controlling that information.

The policy shall apply to all partners and staff of ENABLE.

Objectives of the Policy

The objectives of the policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss.
- Information is true and accurate.
- Information and equipment are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented at an acceptable cost.

- Audit records on the use of information are created and maintained as necessary.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this policy.

The International Standard ISO/IEC 27001:2005 standard specification for Information Security Management defines Information Security as protecting three aspects of information

- CONFIDENTIALITY – making sure that information is accessible only to those authorised to have access
- INTEGRITY – safeguarding the accuracy and completeness of information and processing methods
- AVAILABILITY – making sure that authorised users have access to information and associated resources when required

Legal Obligations

ENABLE accepts its obligations to comply with the laws of the United Kingdom. All staff must be aware that there are legal requirements relating to information that must be met.

The principles of these are detailed below.

- Data Protection Act 1998
- General Data Protection Regulation 2016

Information held electronically that relates to individuals is subject to this Act, which places obligations on those who record and use the personal data and the organisation for which they work.

The Chief Executive Officer (CEO) is appointed Data Protection Officer and is responsible for registration matters with the Office of the Data Registrar, application of the Data Protection Principles and the briefing of all data users within the team.

Freedom of Information Act 2000

The act creates a general right of access, on request, to information held by public authorities. The Funding Bodies for contracts secured by Enable are covered by the Act and have a duty to respond to an information request 20 working days.

Personnel Security Control

The CEO and Operations Manager will ensure that all contracts of employment and any contracts of agency staff include a non disclosure clause.

The CEO and Operations Manager will ensure that security responsibilities are allocated to staff and written into job descriptions and person specifications.

Security training will be provided to all staff as appropriate to their assessed needs.

Physical Security Control

Principle

Resources associated with information processing, such as offices, computer equipment, communications, media and paper based records shall be protected from unauthorised access, misuse, damage and theft.

Access

- As tenants, Enable will ensure satisfactory arrangements are embedded in each location to control access by staff and visitors. This includes signing in books, where appropriate.
- Staff should ensure that no unauthorised visitors tailgate them into the building or office space.

Equipment Security.

- All hardware and software assets held by ENABLE are to be held against an asset register and be uniquely marked as being the property of ENABLE.
- Only staff and third party support staff will be given access to equipment, IT, peripherals and office furniture.
- Equipment, IT, peripherals and office furniture are not to be removed from ENABLE premises without the written permission of The Chief Executive Officer.
- The disposal and storage of equipment is subject to specific security control. Where appropriate, the advice of professional parties is to be sought to ensure effective disposal.
- Users leaving their workstation are to log off the system or lock the system to prevent unauthorised access.
- Secure rooms, including the archive room, not in use should be locked
- Any cupboards, filing cabinets or pigeonholes containing secure data should be locked at all times and only unlocked by authorised persons to access specific records
- Equipment in use in delivery of contracts (i.e. access tokens) should only be used by authorised staff and kept securely at all times

Off Site Working Control

- Managers authorising home/teleworking must satisfy themselves as to security arrangements and ensure that staff are aware of their responsibilities and polices in relation to confidential information.

Security Incidents and Reporting

All security events, weaknesses and incidents must be reported immediately in line with the Information Security Incident Management Policy and Procedure.

Housekeeping

- Users should not store data on their PC hard disk.
- All back up data will be accorded the same level of security as live data and held separately at an off site secure location.
- Data should be reviewed regularly in line with legal requirements.

Business Continuity Planning

A Business Continuity Plan has been produced to ensure the continuation of ENABLE's business in the event of various scenarios occurring.

Implementation

The Chief Executive Officer is the person responsible for the information security of ENABLE. The Operations Manager and Standards Officer will be responsible for the annual review of the policy and where necessary shall undertake reviews to assess the adequacy of implemented security measures including compliance with the policy.

Compliance with the policy is the duty of all partners and staff. In serious cases, failure to comply with the policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence.

All staff have an obligation to report suspected breaches of the policy immediately to the CEO.

In the case of a breach or suspected breach that could affect the security of ENABLE, the Information Security Incident Management Procedure should be applied.

Roles and Responsibilities

The Chief Executive Officer is the nominated Security Officer for ENABLE and shall:

- Develop and manage ENABLE’S security programme.
- Maintain the strategic Business Continuity Plan and advise all ENABLE staff on its implementation.
- Report annually to the Board on the effectiveness of the overall information security programme.

The CEO and Operations Manager

- Create an information security awareness programme to include whole ENABLE briefings training and education.
- Provide information security consulting support for ENABLE.
- Investigate breaches of security, report findings and recommend remedial action.
- Implement a compliance programme to evaluate the effectiveness of the information security programme.
- Assess the risks to the security of the information and the impact of its loss for both short and long periods.
- Employ suitable measures to reduce risks.
- Ensure that equipment is only utilised for ENABLE business.
- Ensure that information is authentic, correct, complete and auditable.
- Ensure that information is backed up regularly and at a frequency commensurate with its usage and is validated.
- Safeguard, maintain and retain all ENABLE records in line with legal retention requirements.
- Ensuring that information exchange with external organisations within or without ENABLE does not compromise the confidentiality of sensitive information, nor does it increase the risk of data corruption.

Users shall:

- Assign a security classification to information where applicable.
- Define who is authorised to access the information on a need to know basis.
- Ensure that information is authentic, correct, complete and auditable.

Review

This policy is to be reviewed on an annual basis by Operations Manager and Standards’ Officer, to take account of changing circumstances, legislation, technology and security risks.

Staff Compliance Agreement

All employed and attached staff must read this policy and sign a certificate agreeing to abide by the requirements laid down in this policy.

The certificate is at Annex A overleaf.

Signed certificates are to be retained in each staff member’s Personnel File.

Should a delivery partner require advice and/or guidance in developing their strategies or operating instructions they should contact the Data Protection Officer – The Chief Executive Officer.

Information Security Policy

Staff Compliance Agreement

I have read and understand
ENABLE'S Information Security Policy
and agree to abide by the requirements laid down in the Policy

Name

Signature

Date

This agreement is to be signed by all personnel working at
ENABLE
and is to be retained in the personnel files