ENABLE
The Voluntary and Community Sector Learning and Skills Consortium

ICT Acceptable Use Policy

Change History

First Published:	16/03/2010	**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	Small changes to wording and referencing	Operations Manager	23 July 2018
13/09/2018	Standards Officer	No Changes	CEO	13/09/2019
21/04/2020	SMT	No changes	CEO	21/04/2021
06/10/2020	BDM	COVID-19	SMT	21/04/2021

Strategic Commitment

Enable's intentions for publishing an ICT Acceptable Use Policy are not to impose restrictions that are contrary to Enable's established culture of openness, trust and integrity. Enable is committed to protecting Enable's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Section 26(1) of the Counter-Terrorism and Security Act 2015 stipulates that we have a duty when exercising our functions, to have due regard to the need to prevent people from being abused or drawn into terrorism.

Internet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol, are the property of Enable. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Enable employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Enable. These rules are in place to protect the employee and Enable. Inappropriate use exposes Enable to risks including: virus attacks, compromise of network systems and services and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporary staff and other workers at Enable, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Enable.

Policy

General Use and Ownership

1. While Enable's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Enable. Because of the need to protect Enable's network, management cannot guarantee the confidentiality of employee personal information stored on any network device belonging to Enable.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Enable is responsible for creating guidelines concerning personal use of Internet systems. If there is any uncertainty, employees should consult their line manager.

3. Enable recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Enable's **Classification and Protective Marking Policy**. For guidelines on encrypting email and documents, go to Enable's **Information Exchange Policy**.

4. For security and network maintenance purposes, authorised individuals within Enable may monitor equipment, systems and network traffic at any time, per Enable's **Audit Policy**.

5. Enable reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet-related systems should be classified as Public, Protected, Restricted or Confidential, as defined by **Classification and Protective Marking Policy**. Examples of each of these types of information are given in the policy. Employees should take all necessary steps to prevent unauthorised access to this information.

2. Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords and user level passwords should both be changed every quarter. See Enable's **Password Procedure**.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging-off the local workstation (control-alt-delete, or by pressing control+alt+end if within the remote desktop environment) when the host will be unattended.

4. Use encryption of information in compliance with Enable's **Classification and Protective Marking Policy**. When sending an e-mail containing personal data or with attachments containing personal data, the Classification and Protective Marking Policy should be taken into consideration. If an e-mail needs to be encrypted, until such time as encrypted mail is available across Enable, the message should be sent from a manager's PC system which would have encryption software to encrypt the email.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the **Acceptable use of Assets Policy**.

6. Postings by employees from an Enable email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Enable, unless posting is in the course of business duties. The disclaimer should also include instructions on actions to take if the mail is received in error. The disclaimer will be added to the end of the signature

7. All hosts used by the employee that are connected to the Enable Internet, whether owned by the employee or Enable, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code, and should inform Line Managers in line with the **Information Security Incident Management Policy.**

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Enable authorised to engage in any activity that is illegal under UK law while utilising Enable-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Enable.

2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Enable or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using an Enable computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any Enable account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to Enable is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.

15. Providing information about, or lists of, Enable employees to parties outside Enable.

16. The Internet must not be used to access sites or download material deemed to be unsuitable. This means the following types of sites:-
    - Pornographic.
    - Online gambling.
    - Racially unacceptable, discriminatory, defamatory or threatening.
    - Illegal.
    - Promotion of extremism and/or radicalisation.
    - Contrary to the strategic aims or principles of Enable.

Prevent Duty

Enable has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or material related to proscribed organisations or material which is at risk of drawing people into terrorism and/or poses a risk of inducing people into making the transition from extremism to terrorism and/or adversely affects the reputation of Enable.

Enable reserves the right to block or monitor access to such material.

Email and Communications Activities

Email use must be compliant with Enable’s **Email Use Policy.** Business emails should contain the e-mail signature, the Communications Officer will provide guidance on style, font, colour and inserting the logo.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorised use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within Enable's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by Enable or connected via Enable's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging

1. Blogging and the use of Social Media by employees, whether using Enable’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Enable’s systems to engage in blogging and use of social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Enable’s policy, is not detrimental to Enable’s best interests, and does not interfere with an employee's regular work duties. Blogging and use of Social Media from Enable’s systems is also subject to monitoring.

2. Enable’s **Classified Data Policy** also applies to blogging and use of Social Media. As such, employees are prohibited from revealing any Enable confidential or proprietary information, trade secrets or any other material covered by Enable’s Confidential Information policy when engaged in blogging and use of Social Media.

3. Employees shall not engage in any blogging and use of Social Media that may harm or tarnish the image, reputation and/or goodwill of Enable and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging and using Social Media or otherwise engaging in any conduct prohibited by Enable’s **Equality and Diversity Policy**.

4. Employees may also not attribute personal statements, opinions or beliefs to Enable when engaged in blogging and whilst using Social Media. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Enable. Employees assume any and all risk associated with blogging and use of Social Media.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Enable's trademarks, logos and any other Enable intellectual property may also not be used in connection with any blogging and use of Social Media activity.

E-Safety - Senior Management will:

- Facilitate training and guidance on Social Media use.
- Develop and implement the Social Media policy.
- Approve account creation to receive completed applications for Social Media accounts

Covid-19

Technology is now widely used to help alleviate the stress and anxiety caused by the Coronavirus pandemic. However, COVID-19 is impacting on individuals' mental health, and problematic internet use (PIU) has and still is increased during the pandemic.

The fear that has resulted from the Coronavirus disease, and the consequences of lockdown has made many people turn to the internet more and more. Because of this, there are several risks associated with internet use, and although this is normally non problematic for most, others find they use or have used the internet without caution, which can lead to distress instead of helping prevent it.

To help diminish the risks of increased use of ICT devices and online activities, and to reduced engagement in usual social interactions and other activities of daily living, Enable recommend that people take time away from the internet by engaging in a physical activity regularly. This not only keeps you healthy, but it also contributes to boosting mood by reducing levels of stress hormones. We also recommend that a daily routine is made, for example, by making an activity schedule for each day and week.

The Government, governmental bodies and industry have made great progress in the quest to make the internet a safer place for young people, children, vulnerable people, and adults alike, but we recognise that risks and dangers remain. Other ways Enable recommend reducing the risks from internet use is:

- not to publish personal information like addresses or phone numbers
- adjust privacy and safety settings to increase security and control the personal data you share. (look for the 'privacy and security' or 'settings' on the app or website).
- review the security settings on your 'smart' devices. If your device is using a default or easily guessable password, change it.
- set up two-factor authentication. This is a free security feature to stop unwanted people getting into your accounts. You will receive a text or code when you log in to check you are who you say you are.
- update your devices. Using the latest version of software and apps
- switch on family friendly filters.
- check firewalls and anti-virus tools are still installed on laptop and computer systems

As a company, we, Enable, will continue to monitor the advice given by the Government, the WHO and PHE, and will update this policy accordingly, when necessary or needed, to reflect the advice given.

Responsibilities and Enforcement

All Staff to abide by the policy.

Line Managers to enforce the policy through performance management processes.

Chief Executive to enforce the policy through Performance Management processes

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Policy Review

This policy to be reviewed every three years by the CEO, Operations Manager and Standards Officer

Definitions

Blogging Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Spam Unauthorised and/or unsolicited electronic mass mailings.

Related Documents

Classification and Protective Marking Policy
Audit Policy
Password Procedure
Remote Access Policy
Classified Data Policy
Email Use Policy
Information Security Incident Management Policy
Information Exchange Policy
Equality and Diversity Policy

Signed:_____

Position:_____

Date:_____