HOET
Heart of England Training Ltd

E-Safety Policy

Introduction

Heart of England Training recognises the benefits and opportunities which new technologies offer to teaching and learning. Internet access is provided to all learners and staff encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

The accessibility and global nature of the internet and different technologies mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the organisation and support staff and learners to identify and manage risks independently. The company does all that it can so that learners and staff stay safe online and is fully committed to the Every Child Matters, 'Working Together to Safeguard Children' and the Government Prevent Duty Counter-Terrorism and Security Act 2015 agenda.

Scope

This policy applies to everyone who have access to the company IT systems, both on the premises and remotely. The e-safety policy applies to all use of the internet and electronic communication devices such as e-mail, mobile telephones, social networking sites, instant messaging and any other systems that use the internet for connection and providing information.

Definition

The term e-safety is defined for the purpose of this policy as the process of limiting the risks when using internet, digital and mobile technologies through a combined approach to policies, procedures, infrastructure and training.

Examples of e-safety risks

- exposure to age-inappropriate material
- exposure to inaccurate or misleading information
- exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- exposure to illegal material, such as images of child abuse
- exposure to extremist or radical views/ materials

Examples of e-safety contact

- grooming using communication technologies, leading to sexual assault and or child prostitution
- grooming using extremist or radical views/materials for the purpose of illegal activity

Examples of e-safety commerce

- exposure of minors to inappropriate commercial advertising
- exposure to online gambling services
- commercial and financial scams

Examples of e-safety culture

- Bullying via websites, mobile telephones or other forms of communication device
- Downloading of copyrighted materials e.g. music and films

Roles and responsibilities

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their manager. All staff are required to cover e-safety guidance when using online technology with learners and staff and learners must act safely and responsibility at all times when using the internet and or mobile technologies. They are expected to be aware of and act in line with other relevant company policies and follow reporting procedures where worried or concerned about an e-safety incident they believe has taken place.

Control measures

Heart of England Training will do all that it can to make sure the company network is safe and secure. Every effort will be made to keep security software up to date and to comply with Data Protection regulations to include GDPR.

Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers and work stations to prevent accidental or malicious access of systems and information. Digital communications, including email and internet usage over the organisation's network will be monitored in line with other company policies and what is considered acceptable use. Only access through the company website is allowed when working remotely.

Incidents and response

Where an e-safety incident is reported to the organisation, the matter will be dealt with very seriously. Heart of England Training will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If anyone wishes to report an incident, they can do so to their trainer, manager or the company Safeguarding Lead. Incidents/breaches regarding data must be reported to the company Data Controller immediately for ICO notification.

Failure to comply with the above policy may result in disciplinary action that may lead to dismissal. Where conduct is considered illegal, Heart of England Training will report the matter to the police.

This policy is reviewed annually by the company directors.

Version: 5
Prepared by: Directors
Approved by: Governors

Effective date: September 2022
Review date: August 2022
Date to be reviewed: July 2023