# E-SAFETY POLICY

## Policy Number: OPG022

Version 1
Date released: 19.12.2018
Date reviewed: 24.11.2021
Reviewed by: Kate Temple-Brown
Date to be reviewed: 01.11.22
Author: Andrea Satterthwaite

**BACKGROUND**

The Opportunity Group recognises the benefits and opportunitieswhich new technologies offer to teach and learning. We provide internet accessto all learners attending our short courses and staff encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the company while supporting staff and learners to identify and managerisks independently and with confidence. We believe this can be achieved through a combination of security measures,
training, guidance and implementation of our policies.

In continuation of our duty to safeguard learners we will do all thatwe can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

The policy applies to all users/all learners and staff of TheOpportunity Group
who have access to our IT systems, both on the premises and remotely.
Any user of The Opportunity Group's IT systems must adhere to this policy.
Thee-Safety Policy applies to all who use of the internet and forms of electronic communication such as email.mobile phones and social media sites.

**Roles and Responsibilities**

There are clear lines of responsibility fore-safety within the company. The first point of contact should be the Quality and Compliance Specialist. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All coaches and assessors are required to offerguidance one-safety to their learners and to read through and report incidents in line with the policy. When informed about an e-safety incident. staff members must take care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be the Quality and Compliance Specialist. All parties should know what procedure istriggered and how this will be followed up. Where management considers it appropriate, the Designated Safeguarding Officer maybe asked to intervene with appropriate additional support from external agencies.

**e-Safety Officer/Designated Safeguarding Officer**

The Designated Safeguarding Officer is responsible for keeping up todate with new technologies and their use, as well as attending relevant training. They will be expected to complete, review and update thee-Safety Policy, deliver staff development and training, record incidents, report any developments and incidents to the Leadership and Management team and liaise with the local authority and external agencies to promote e-safety.

**Learners:**
Learners are responsible for using The Opportunity Group's ITsystems and mobile devices in accordance with the company requirements Learners must act safely and responsibly always when using theinternet and/or mobile technologies. They are responsible for attending e-safety lessons as part of the curriculum and are expected to know and act in line with other relevant company policies e.g. mobile phone use. sharing images. cyber- bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident hastaken place involving them or another member of the company.

**Staff:**
All staff are responsible for using The Opportunity Group's IT systemsand mobile devices in accordance with the company Acceptable UsePolicies.

- Staff are responsible for attending staff training on e-safety and displaying a model example to learners always throughembedded good practice.
- All digital communications with learners must be professional always.
- All staff should apply relevant company policies and understand the safeguarding incident reporting procedures.
- Any incident that is reported to or discovered by a staff member must be reported to the Designated SafeguardingOfficer and/or line manager without delay.

**Security**
The company will do all that it can to make sure the companynetwork is safe and secure. Every effort will be made to keep security software up to date.

Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of company systemsand information. Digital communications, including email and internet postings, over the company network will be monitored in line with the IT, Computer Usage Policy.

**Behaviour**
The Opportunity Group will ensure that all users of technologiesadhere to the
standard of behaviour as set out in the Information, IT andCommunications Security Policy NO GRAD021.
The company will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful always. Any reported incident of bullyingor harassment or other unacceptable conduct will be treated seriously and in line with the company and staff disciplinary codes.

Where conduct is found to be unacceptable, the company will deal with the matter internally. Where conduct is considered illegal, the company will report the matter to the police.

**Communications**

The Opportunity Group requires all users of IT to adhere to Use ofInternet. Email & Social Media Policy which states clearly when email, mobile phones, social media sites, games consoles, chat rooms, video conferencing and web cameras may be used during the day.

**Use of Images and Video**

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach ofcopyright or other rights of another person (e.g. images rights orrights associated with personal data).

This will include images downloaded from the internet and thosebelonging to staff or learners.

All learners and staff should receive information on the risks whentaking, downloading and posting images online and making themavailable to others. There are risks where personal images of themselves or others are posted onto social networking sites.

This includes photographs of learners and staff as well as using thirdparty images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

**Personal Information**

Personal information is information about a living person, The Opportunity Group collects and stores the personal information oflearners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on.

The company will keep that information safe and secure and will not pass it onto anyone else without the express permission of the learner/parent/ carer. No personal information can be posted to the company website/without the permission of the Designated Safeguarding Officer unless it is in line with our Data Protection Policy No 112. Only names and work email addresses of (senior) staff will appear on the company website/no staff/no learners' personal information will be available on the website without consent. Staff must keep learners' personal information safeand secure always.

No personal information of individuals is permitted offsite unless the member of staff has the permission of Designated Safeguarding Officer. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period. Where the personal data is no longer required, it must be securely deleted in line with the Data Protection and Confidentiality policy.

**Education and Training**

With the current unlimited nature of internet access, it is impossiblefor the company to eliminate all risks for staff and learners. It is our view therefore, that the company should support staff and learnersstay e-safe through

regular training and education.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. Theywill also be encouraged to respect the copyright of other parties andto cite references properly.

Staff will take part in e-safety training before beginning a new company year. This will be led by the Designated Safeguarding Officer and will take the format of a workshop, allowing tutors' hands-on experience. Further resources of useful guidance and information will be issued to all staff following the session. Each member of staff must record the date of the training attended ontheir CPD calendar.

**Incidents and Response**

Where an e-safety incident is reported to the company this matter will be dealt with very seriously. The company will act immediatelyto prevent. as far as reasonably possible, any harm or further harm occurring.

If a learner wishes to report an incident. they can do so to their tutoror to the company Designated Safeguarding Officer.

Where a member of staff wishes to report an incident. they mustcontact their line manager as soon as possible.

Following any incident. the company will review what has happenedand decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved, or the matter may be resolved internally depending on theseriousness of the incident.