5 E Ltd
Selby Centre
Selby Road
London N17 8JL
Tel: 020 8885 3456
Fax: 020 8808 9977
E-mail: enquiries@fivee.co.uk
Website: www.fivee.co.uk

E-Safety Policy

Introduction

5E Ltd hereinafter referred to as the organisation recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and 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 organisation while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read alongside other relevant organisation policies e.g. Safeguarding, ICT policy, Equality and Diversity policy and Disciplinary Protection."

Creation, Monitoring and Review

We have different stakeholders who have contributed to the creation and review of this policy include the e-Safety Officer/Safeguarding Officer (DSP), a senior line manager, IT Security Manager, members of teaching/support staff and learners.

Policy Scope

The policy applies to all users/all learners and staff/all members of the organisation who have access to the organisation IT systems, both on the premises and remotely. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites etc.

Roles and Responsibilities

The health and safety of staff and learners is encompassed by our Safeguarding, Health & Safety and Equal Opportunities policies and procedures. Our Safeguarding Policy is not restricted to children and vulnerable persons, but aims to protect all our learners from harm including potential harm form the internet, social networks and other electronic media.

Designated safeguarding person within the organisation aims to ensure that policies are implemented and that regular monitoring takes place. All learners and staff should be made aware of safeguarding policies and abide with the Acceptable Use Policy Agreement (Appendix A and C respectively).

All users should be encouraged to use computers and the internet responsibly and to understand the consequences their actions could have on themselves and others.

The policy encompasses other technologies, including the safe use of mobile phones, Personal

Digital assistants (PDA's), and safe use of social network sites.

Accountability and responsibility for safeguarding and E-Safety

There are clear lines of responsibility for e-safety within the organisation. The first point of contact should be the E-Safety/Safeguarding Officer. DSP- Sailesh Solanki- 07904957799.

Organisation's Responsibilities

- To ensure that this policy is distributed to all members of staff.
- To ensure Learners/Employers/Parents, Guardians or Carers/Visitors and other clients are aware of our e safety procedures
- Where appropriate, inform Parents/Guardians/ Carers of this policy and ask for confirmation of understanding via completion of the use of internet agreement (Appendix B)
- To regularly review the content of the policy to take account of developing technology.
- To identify and install suitable content filtering and audit software where Internet access is provided, in addition to any filtering service offered by the Internet Service Provider (ISP).
- To provide guidance and training for all staff that will be responsible for the delivery or supervision of internet based learning.
- To put in place mechanisms for monitoring responsible ICT use in establishments.
- To reinforce the understanding of staff and learners that material on the Internet is also subject to copyright legislation.
- To review existing policies including safeguarding Policies and codes of practice to reflect the threat of technology abuse.

Tutors/Assessors have the following responsibilities:

- Provide information about learner safety and security related to the Internet and electronic communications to all learners via induction.
- To ensure that all internet access is supervised
- Ensure learners, visitors and non-organisation employees are not given passwords and access to staff intranet and Management information systems and the internet without authorisation from the HR, Line Manager and IT Manager.
- To provide learners, staff and any other adults an Acceptable Use Agreement, (Appendix A & C) where they must confirm acceptance of its terms, before being allowed Internet access.
- To have a system of immediate sanctions for dealing with improper use of ICT equipment as part of this policy.
- To connect to the Internet only through the filtered network service.
- To ensure staff and learners are aware that their Internet activity is monitored by organisation
- To follow organisation policy on the use of photos and personal details on the organisation Website included in the Acceptable use Policy Agreement.
- To follow organisation policy on the use of video conferencing and/or webcams with/by learners and to reinforce this policy with learners.
- To reinforce the understanding of learners that material on the Internet is also subject to copyright Legislation and to reinforce that plagiarism of material from the internet is not acceptable unless referenced within the main text or Bibliography.

In addition all employees of organisation must:

- not have in his/her possession at any time illegal materials/images in electronic or other format;
- not have in his/her possession inappropriate materials/images on organisation premises;
- not download or access illegal images at anytime or in any place;
- not access inappropriate sites or download inappropriate materials on organisation premises;

- ensure that he/she is fully aware of this and other related policy and ICT guidelines and adhere to them
- ensure all communications with learners must be justified in terms of learning and teaching.

In any event this should be carried out in a professional manner using an official organisation email address and in strict compliance with organisation policies;

- not engage with any learners via contact/web cam sites (for example chat rooms, message boards and newsgroups) for any purpose other than training and not engage in communication with individuals under 18 or are deemed to be vulnerable using this media or with whom he/she is in a position of trust. Staff must seek guidance from their line manager if they feel there is a legitimate benefit in pursuing this type of media with persons over the age of 18.

Responsibilities of learners:

- To have a responsible attitude to the use of ICT equipment and internet /email provision.
- To agree to and follow Policies and Guidelines on acceptable use and to report any misuse or suspected misuse by others, including bullying and harassment via electronic means.
- To follow the Internet Safety Rules' (Appendix B)
- Learners should not use USB or other devices without the permission of a organisation member of staff on any organisation laptops or electronic devices to avoid the transfer of viruses and unsuitable material.
- Learners must ensure these devices are free of viruses before use.

Guidance to learners

Staff should give information to learners on Internet safety which includes:

- Making sure they never tell anyone they meet on the Internet personal details such as their home address, phone numbers, photos or bank details
- Make sure that they never tell anyone they meet on the Internet their employer's name or phone number.
- Never arranging to meet in person someone they first met online.
- Ensuring they understand that not everything they read online is true.

Guidance to visitors

On the rare occasions where visitors have access to our internet and ICT systems the same responsibilities for learners apply.

Visitors must obtain authorisation to have access to the internet and internal ICT systems but must not be given access to the staff intranet and MIS systems unless there is a legitimate reason.

Supervision of Learners

All staff have a responsibility to maintain the safety of Learners.

The following guidance should be adhered to when supervising learners:

- Learners should never be left unsupervised when using the Internet.
- Computers should be within sight of the teacher or tutor.
- For senior pupils and mature students, the teacher, tutor, or responsible adult, may supervise indirectly but should still monitor learner activities.
- Employers, who have learners on work placement schemes or have employees who have access to the Internet, should be informed of this policy and should not allow them to have unsupervised unfiltered Internet access.
- Rules outlining the use and restrictions when using the internet should be available to all learners if they have access to the internet. (Internet Safety Rules, Appendix D).

Acceptable Use Policies

Learners, staff and any other adults with Internet access must sign the Acceptable Use Agreement (Appendix A and C respectively).

Use of the Internet

The following internet procedures must be followed by all users to ensure safe and responsible use of the web. It should always be remembered that visits to sites are recorded and can be traced back to the user.

- Staff should inform their line manager, and learners should inform their tutor or employer immediately if any abusive, threatening or offensive sites are discovered.
- Care should be taken that any material published to the web does not breach any of the guidelines in this policy or other policies relating to data protection, copyright and Intellectual Property Rights (IPR).
- Personal information should never be divulged to others.
- Use of an adult's credit card details should not take place by learners when learners are in the care of organisation.

Use of E -mail

The following procedures must be followed by all users including staff to ensure safe and responsible use of e-mail. It should be remembered that e-mails are recorded, can be traced back to the sender and can be legally binding.

- Users should change passwords regularly and should not divulge them to others.
- Learners should inform their tutor/assessor or employer immediately if any abusive, threatening or offensive e-mails are received.
- Inform their Tutor/assessor or employer immediately if an e-mail or attachment generates a virus warning.
- Staff may make personal use of the Company's internet and e-mail facilities outside the normal working day when this is necessary. However, staff are encouraged to use their own personal email accounts for this purpose on all other occasions. Personal use of the organisation's email accounts is subject to the same rules that apply at other times.
- Staff should be aware that their e-mail is filtered and no organisational e-mail accounts are private.
- The contents of learner or staff e-mail accounts or details of online activity may be checked at any time.
- Staff should never use organisation Internet and e-mail accounts to send private confidential information or provide credit card details.
- Staff should be aware that their e-mail use and internet activity is monitored and recorded.

Staff working with young people should ensure that:

- They do not engage in private/personal correspondence or communication with a student or pupil. (This includes texting and Media Messaging e.g. MSN Messenger, Social networks e.g. Facebook, Skype etc)
- They take care in communicating with learners via e-mail to ensure the correspondence is for training and assessment purposes only. Staff must ensure their correspondence is non discriminatory or could cause offence. Correspondence must be on a professional basis and must not be of a personal nature.

Use of Internet Newsgroups

Internet newsgroups can be a valuable means of exchanging information on specific topics. Some newsgroups have been developed specifically for educational purposes and are moderated to filter out any inappropriate material. Newsgroups which are not moderated are totally inappropriate for educational purposes and must not be used.

Using File Transfer Protocol (FTP) for downloading software

Staff and Learners must not download or attempt to download software such as drivers and application software. Such activities are restricted by the Network Administrator. Permissions to download software must be sought by staff from the Managing Director.

Use of Internet Relay Chat (IRC) and Instant Messaging

IRC allows users to speak to other users using a microphone linked to the computer or via visual interaction such as Skype or MSN messenger typed messages can also be sent in this way. Organisation training supports the use of these technologies as a teaching and assessment tool. However, organisation does not support the use by learners and staff of "chat rooms" and these technologies while training and/or assessment is being undertaken unless it is part of their training programme.

- Learners should be given guidance on safe use of "chat rooms" as part of our Safeguarding policy. A number of chat rooms are available which are safe for learners to use as they are closely monitored and restrict access.

For information which could be discussed with learners, www.chatdanger.com has examples about the dangers of chat rooms plus guidelines for safe chatting.

Virus Protection

All organisation computers, used for access to the Internet, are installed with anti-virus software. Introducing viruses to computers, or attempting to break through network security is a serious offence, and users should be aware of the issues and the risks.

- Any user who suspects the presence of a computer virus must alert their tutor/ assessor or, in the case of staff, their line manager immediately.

Copyright

Copyright rules apply to material available over the Internet, and will generally be subject to the same level of protection as material in other media. Although there are no specific exceptions from copyright material on the internet, those relating to Fair - dealing for the purposes of non – commercial research or private study may apply. Users should be aware of copyright notices on websites setting out how the material may be used and how to obtain permission.

Guidelines on the use of material off the internet are as follows.

- Learners and staff should acknowledge sources within the document or as part of a bibliography.
- Users should not assume that educational use of material is permitted, without first checking with the author. (Web-based resources may themselves have been published without the appropriate permissions. Therefore, any subsequent use of such material may also be illegal.
- Staff should be aware that any material they publish on the organisation website may be used by others without unauthorised use.
- Publishing other people's material without their explicit permission is a breach of copyright; this applies to use of images from the internet used within a document.
- Showing and accessing websites in a lesson is not a breach of copyright, but copying an entire page into, without appropriate permission for own use e.g. a PowerPoint presentation
- Copying material from the Internet and printing it for pupil use could be a breach of copyright. Using it as part of a larger document without appropriate permission would be.
- Copyright laws vary between countries.

Website Development

Access to the organisation website is open to all. However, the authority to be able to add information to the website is restricted to organisation staff and monitored by the Senior Management Team. Where a picture or image of a learner, client or a member of staff is used, permission to use this image will be sought from the source before use, and from parents/carers if appropriate. The organisation is aware that images can be downloaded from the internet including

websites by others without the authority or permission to do so. The organisation has a responsibility to protect the young people and vulnerable adults in their care and will consider the risks involved in any information which appears on our website. Our commitment to ensuring a person's rights and safety are not compromised include:

- Ensuring names of young and vulnerable persons should not appear in websites.
- Photographs of individual young people and vulnerable adults should not be posted in websites.
- Photographs of groups of young people may be posted but only with written parental permission for all members of the group.
- Ensuring parents of children are fully informed of these procedures and the reasoning behind them.

Mobile Phones

PDAs and Digital Cameras. Due to the issues of personal safety, organisation does not ban the use of mobile phones by learners and expects all staff to carry mobile phones issued by the company for their own safety. However the following rules should be followed to minimize the risk of inappropriate or illegal use of these devices while learners are undertaking training and assessment with organisation.

- Mobile phones must be completely switched off during all training and assessment sessions unless special permission is granted by the tutor. Devices may be put on "silent" or "vibrating".
- Use at lunchtime and intervals may be permitted where the rules of safe use are followed.
- Inappropriate use of text messaging is not allowed at any time by staff and learners.
- Digital video or still cameras should only be used as part of a planned lesson with teacher supervision unless the learner is using video or photographic evidence as part of their evidence for assessment.
- No photographs, video or sound recordings can be taken without the express approval of the subject, whether learners or staff.
- Where a learner provides photographic or video evidence where others are in shot, permission should be sought from those persons by the Learner, or preferably by the tutor beforehand.
- Bluetooth technology should not be used to transfer images at any time by staff or learners. Such images can be picked up by other Bluetooth enabled devices belonging to others in the vicinity.
- These rules apply to any equipment offering the same functions as mobile phones.
- Serious cases of intimidation and bullying with such devices will be referred to the police.

Videoconferencing

The use of video conferencing by organisation is limited, but has the potential to increase. The procedures for video - conferencing are the same for displaying information about learners on a web site.

It is possible that an unauthorised person could record sound and vision externally.

- Staff should ensure that learners and other clients are informed that they should not divulge personal information in a conference call including full contact details.

Personal Information

Personal information is information about a particular living person. The organisation collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The organisation will keep that information safe and secure and will not pass it onto anyone else without the express permission of the subject.

No personal information can be posted to the organisation website without the permission of the E-Safety Officer and the Data Controller. Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. No personal information of

individuals is permitted offsite unless the member of staff has the permission of E-Safety 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.

All organisation mobile devices such as a laptop, USB (containing personal data) require to be encrypted, password protected and signed out by a member of the IT staff before leaving the premises.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection Policy."

With the current unlimited nature of internet access, it is impossible for the organisation to eliminate all risks for staff and learners. It is our view therefore, that the organisation should support staff and learners stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

Learners will attend e-safety lessons in a session. The first of these will take place on the day of their induction. Issues associated with e-safety apply across the curriculum and learners would receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Learners would know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. The organisation e-Safety Rules will appear when users log on to the organisation network and these rules are highlighted in posters and leaflets around IT areas and work stations.

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

E-safety training would be included in the organisation's induction procedure. This will be led by the E-Safety Officer/HR. Any new or temporary users will receive training on the organisation IT system at the time of their induction,

Prohibitions

The following activities are prohibited by all users

- Download or attempt to download software, applications, etc., on Laptops or any hardware provided by organisation unless permission is expressly given to organisation staff by the Tutor.
- Use of chat rooms, social networks, texting, use of emails for personal use while training and assessment is being undertaken. Staff must not engage in the use of these technologies for their own personal use in working hours.
- Use of the Internet to harass, offend or bully any other person;
- Use of the Internet for any inappropriate or illegal purpose;
- Use of the Internet for transmission of threatening, offensive or obscene material;
- Use of the Internet for transmission of material from any criminal organisation;
- Use of the Internet for the transmission of viruses or unlicensed software.

17. Actions and Disciplinary procedure

The organisation operates a zero tolerance policy when staff and learners are placed at risk through their activities and the activities of others. Noncompliance with this and other related policies will not be tolerated. Failure of staff, learners and others to comply with this policy may result in the following:

- Removal and revoking of permissions to use ICT resources for the purpose of training and assessment provided by organisation.
- Invoking and applying the learner disciplinary procedure.
- Invoking and applying the staff disciplinary procedure.
- Referral of allegations and evidence of criminal activity to the Police.

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All teaching staff are required to deliver e-safety lessons to classes. When informed about an e-safety incident, staff members must take particular 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 Sailesh Solanki- 07904957799 or the Centre Manager. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the appropriate authorities may be asked to intervene with appropriate additional support from external agencies.

Incidents and Response

Where an e-safety incident is reported to the organisation this matter will be dealt with very seriously. The organisation will act immediately to 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 tutor, Centre Manger or to the organisation e-Safety Officer. Where a member of staff wishes to report an incident, they must contact their line manager/E-Safety Officer as soon as possible. Following any incident, the organisation will review what has happened and 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 the seriousness of the incident.

Feedback and Further Information

The organisation welcomes all constructive feedback on this and any other organisation policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact Mr Sailesh Solanki our e-Safety Officer at sailesh@fivee.co.uk or 07904957799. Additional Resource- Appendix A E- Safety Guide.

Review of policy

This policy was reviewed in June 2021. The next review is expected in June 2022. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

If you would like this document in larger print, please contact Human Resources Dept.