Approved by Company Director: .....
Date:

E-Safety Policy

1. Introduction

This e-safety policy should be read in conjunction with other relevant Company policies to which it refers e.g. Safeguarding Policy, Information Security Policy, Anti Cyber Bullying and Disciplinary Policy.

Skills UK 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 Company 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.

2. Policy Scope

The e-Safety Policy applies to all users, all learners and staff of Skills UK, who have access to the Company IT systems, whether on the premises or remotely. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phone, social media sites and use of images/video of the Company's staff or learners.

3. Roles and Responsibilities

There are clear lines of responsibility for e-safety within the company. The first point of contact should be Craig Flynn or Eric Robinson, the e-Safety/Safeguarding Officers. 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 and make learners aware of the company reporting procedure. 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 Craig Flynn or Eric Robinson, Safeguarding Officers. 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 child protection officer may be asked to intervene with appropriate additional support from external agencies.

- **E-Safety Officer:**
  The e-Safety Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. He will be expected to, complete, review and update the e-Safety Policy, deliver staff development and training, record incidents, report any developments and incidents to the Directorate and liaise with the local authority and external agencies to promote e-safety within the company.

- **Learner:**
  Learners are responsible for using the company IT systems and mobile devices in accordance with the college E-safety Policy and e-Safety Rules. Learners must act safely and responsibly at all times when using the internet and/or mobile technologies. They are responsible for completing e-safety lessons as part of the curriculum. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another learner/staff member.

- **Staff:**
  All staff are responsible for using company IT systems and mobile devices in accordance with the Company's Information Security and the e-Safety rules. Staff are responsible for completing staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times and be carried out in line with the company's Information Security Policy. Online communication with learners is restricted to the company network.

All staff should apply relevant company policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the e-Safety Officer and the Directorate without delay.

Staff will take part in annual Safeguarding training as a minimum. Each member of staff must record the date of the training attended on their CPD record.

Any new or temporary users will receive a new password or temporary password and will be required to accept and agree to the Company Information Security Policy and sign the confidentiality agreement before they logon to the Company network.

5. Security

The Company will do all that it can to make sure it's network 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 systems and information. Digital communications, including email and internet postings, over the Company network, will be monitored in line with the Information Security Policy; available on the Company intranet, under Policies.

6. Behaviour

Skills UK will ensure that all users of technologies adhere to the standard of behaviour as set out in the Information Security Policy, which they agree to each time they logon to the Company network. The Company will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times.

Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the learner and staff disciplinary codes and Anti Bullying Policy.

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.

7. 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 of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

Skills UK teaching staff will provide information to learners on the appropriate use of images. This includes photographs of learners and staff as well as using third party 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.

Use of photographs of activities on the Company premises should be considered carefully. Learners sign a consent form during the application process, either allowing or withdrawing consent for the Company's use of a learner's image. Approved photographs should not include names of individuals without consent.

8. 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 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 personal tutor or to the Company Safeguarding Officers.

Where a member of staff wishes to report an incident, they must contact Eric Robinson or Craig Flynn without delay. Following any incident, the Company 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. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

9. Feedback and Further Information

Skills UK welcomes all constructive feedback on this and any other company 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: Lynne Shetliffe, Company Director at lynnes@skillsuk.org.

RELATED POLICIES:

P034 - Information Security Policy
P029 - Anti Cyber Bullying Policy
P021 - Safeguarding Policy
P045 - Disciplinary and Dismissal Procedure
P025 - Learner Conduct and Performance Policy and Procedure

Appendix 1

LEARNER E-SAFETY STATEMENT

- I will not visit sites which contain items that are illegal, defamatory, pornographic or in any way offensive.
- I will observe the rules and laws regarding copyright and plagiarism.
- I will not download files to any Company computer.
- I will observe the requirements of the Data Protection Act 1998 and take appropriate steps to protect all personal data.
- I will report any information that I come across which makes me feel uncomfortable or unsafe to my Personal Tutor or a Safeguarding Officer.
- I agree never to write or send malicious or offensive e-mails and accept that offenders will be reported to, a Safeguarding Officer or the Directorate; depending on the severity of the incident.
- I understand that downloading and/or distributing offensive/illegal materials will lead to exclusion and possibly the involvement of the police.
- I agree to use photographs and video clips only with the specific permission of staff and learners and only for educational purposes.
- I understand that if I am found to be involved in on-line bullying, that this will be dealt with in line with the Company's bullying policy.
- I will never give my log in details to anyone else or attempt to access the network using a log in that is not my own.
- I will never slander staff, other learners or the company on a social networking site, e.g. Facebook, Twitter, Snapchat etc.

I confirm that I will abide by the company's e-safety rules whilst using Skills UK Ltd ICT equipment during my course of study. I understand that failure to comply with these rules will result in disciplinary action being taken against me.

Name Signed

Date