E-Safety Policy

SBC Training 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 order to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

Policy Scope

The policy applies to all learners and staff who have access to SBC Training's IT systems, both on the premises and remotely. In addition, Acceptable Use Policies (AUP), for staff and learners, are introduced to them at induction. A link is available for learners to view their AUP on the SBC Training's computers' desktop and network, and the staff version is on the K:Drive. The E-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media etc.

Roles and Responsibilities

There are clear lines of responsibility for e-safety within SBC Training. Although all staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager, any incidents relating to e-safety should be reported to the responsible people (see end of document for current responsibilities). When informed about a learner 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 their trainer. 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. Incidents should be recorded on the Incidents/Accidents form.

Staff with Responsibility for E-safety:

Those responsible for e-safety keep up to date with new technologies and their use, as well as attending relevant training. They will be expected to lead on e-safety; complete, review and update the E-Safety Policy and AUPs; deliver staff development and training; record incidents; report any developments and incidents to Senior Management.

Learners:

Learners are responsible for using SBC Training's IT systems and mobile devices in accordance with the E-Safety and AUP, which will be introduced at induction. Learners must act safely and responsibly at all times when using the internet and/or mobile technologies. Throughout the learners' programme, a number of e-safety issues will be addressed, e.g. mobile phone use, sharing images, cyber-bullying etc. Learners are encouraged to report any instances which cause worry or concern, or where they believe an e-safety incident has taken place involving them or another with whom they learn or work.

Staff:
All staff are responsible for using SBC Training's IT systems and mobile devices (including their own devices, if applicable) in accordance with the AUP and the E-Safety Policy. Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

Digital communications with learners, and all others, must be professional at all times.

All staff should apply relevant e-safety policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be relayed to those responsible for e-safety without delay, following completion of an Incident/Accident form.

Security
SBC Training will do all that it can to make sure its 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 SBC Training's systems and information. There is the facility for all digital communications, including email and internet postings, over the SBC Training network, to be monitored.

Risk Assessment
In making use of new technologies and external online platforms, this policy will be re-evaluated by the Senior Team as part of the quality and equality and diversity procedure.

Behaviour
SBC Training will ensure that all users of technologies adhere to the standard of behaviour as set out in the AUP.

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

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. All learners and staff receive training on the risks when taking, downloading and posting images online and making them available to others. 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.

Personal Information

SBC Training collects and stores the personal information of learners and staff regularly, e.g. names, dates of birth, email addresses, assessed materials and so on. SBC Training 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 SBC Training's website/without appropriate permission. Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be secure. 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.

SBC Training's mobile devices, such as laptops, USBs (containing personal data) etc., are required to be encrypted/password protected.

Where personal data is no longer required, it must be securely deleted, as appropriate, or in line with the organisation's retention procedures.

Education and Training

With the current unlimited nature of internet access, it is impossible for SBC Training to eliminate all risks for staff and learners. It is our view therefore, that SBC Training should support staff and learners to 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.

E-safety will be addressed at induction and throughout the learners' programmes. Issues associated with e-safety apply throughout learners' programmes and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Learners should also 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. A link to SBC Training's ICT AUP for Learners will appear when users log on to SBC Training's network and these rules, along with e-safety guidelines, are highlighted in posters around IT areas and work stations. Within relevant 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.

Staff will take part in mandatory e-safety training and staff will be regularly updated on e-safety requirements. Further resources or useful guidance and information will be issued to all staff. Each member of staff is encouraged to record training attended on their CPD calendar.

Any new staff will receive training on SBC Training's IT systems, from the responsible person. Induction paperwork is signed accordingly as proof.

Incidents and Response

E-Safety Policy

Where an e-safety incident is reported to SBC Training it will be dealt with very seriously. SBC Training 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 trainer or to those responsible for e-safety. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, SBC Training 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.

Current responsible person: Alex Danells