E-Safety Policy

Overview

Welcome Skills takes all learners and Welcome Skills' staff e-safety very seriously. E-Safety encompasses not only internet technologies but also a full range of electronic communications, such as mobile phones and wireless technology. It highlights the need to educate all learners about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Internet use is embedded in the learning experience and is a necessary tool for both learners and staff.

Welcome Skills has a duty to ensure that learners have access to quality internet access as part of their learning experience and learners should always have an entitlement to safe internet access. The use of these exciting and innovative tools in the learning environment and at work and home has been shown to raise educational standards and promote learner progression. However, the use of these new technologies can put learners at risk within and outside the learning environment. Some of the dangers they may face include: -

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is used in conjunction with other policies (e.g. Safeguarding and Prevent).
This policy applies to all Welcome Skills learners and staff.

Using the Internet

Learners will be taught what internet use is acceptable and what is not and given clear objectives for internet use along with advice on the use of other new technologies.

Learners will be taught about effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

DOCUMENT NAME/LOCATION	Date Produced	Version Number	Authorised By:	Document review date
E Safety Policy	June 2021	1	K.Hussin	May 2022

Managing Internet Access

If a learner receives an offensive or bullying e-mail, they must immediately inform their tutor or another member of staff who will then inform the Safeguarding/Child Protection Officer.

Photographs/videos will not be used for marketing purposes e.g. website, newsletter without obtaining the learner's permission and that of the parent/carer where the learner is under 18. The purpose of using the photograph/video will always be made clear.

Learners must not reveal personal details of themselves or others in e-mail communications.

If Welcome Skills staff or a learner discover a workplace is unsuitable, it must be reported immediately to the Safeguarding Officer.

Personal data will be recorded and processed according to GDPR.

Employers employing learners will be given a copy of our E-safety Policy which they must adhere to, unless Welcome Skills review their own policy as satisfactory.

Staff using laptops and mobiles externally must ensure they have no learner personal data stored without the learner permission (e.g. contact information). Laptops must always be stored securely when outside of Welcome Skills and must NEVER be left unattended, for example, left on view in cars.

Other Recent Technologies

Mobile phones must not be used in training rooms unless specifically allowed, to support learning and approved by the trainer. The sending of abusive or inappropriate texts will be classed as misconduct.

Emerging technologies will be researched for educational benefit and a full risk assessment will be carried out before use is approved e.g. Facebook.

Communications

Learners will receive training on E-safety and the E-Safety Policy will be displayed in all training rooms, in which learners have access to IT equipment. Learners under 18 who are employed and undertaking qualifications will receive e-safety training on induction.

All Staff will be given a copy of the E-Safety Policy which will also be stored in the shared folder. New staff will be given a copy on induction.

All Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential as per the 'Code of Conduct'.

Acceptable Social Networking

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

All staff should be aware of their professional reputation and that of Welcome Skills when online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately, as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc. online; would you feel comfortable about a colleague, or learner, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made.

All staff must be aware that as professionals, it is necessary to be cautious to ensure that the content we post online does not bring Welcome Skills into disrepute. If you have a social networking account, it is advised that you do not accept learners as "friends" on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. If you have a pre-existing relationship with learners please be mindful of the above information when liaising with them. Inform your line manager of any concerns, or conflict of interest, such as criticism or inappropriate content posted online.

Roles and Responsibilities

The Senior Management Team

- The Senior Management Team are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by reviewing regular information about e-safety incidents and monitoring reports.
- The Managing Director is responsible for ensuring the safety (including e-safety) of Welcome Skills staff, learners, though the day to day responsibility for e-safety will be delegated to the Safeguarding/Prevent Officer.
- The Senior Management Team are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Management Team will receive regular monitoring reports on e-safety from the Managing Director.
- The Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Managing Director

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policy / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with ICT technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- reports regularly to Senior Management Team.

Staff, are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current e-safety policy and practices.
- they report any suspected misuse or problem to the Managing Director for investigation / action / sanction.
- digital communications with learners should be on a professional level and only carried out using official systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- Learners understand and follow the e-safety policy.
- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons and other activities.
- they are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement policy with regard to these devices.

General

This Policy should not be read in isolation but is designed to be read in conjunction with Welcome Skills' Equality and Diversity Policy, Prevent and British Values Policy, Health and Safety Policy, Conflict of Interest Policy and Safeguarding Policy.