Acceptable Usage Policy – Learners Using PC/Laptop

Learners – Please ensure you read and understand this policy.

Computer misuse

Some learners will have access to computers/laptops during the course of their learning. Abuse of the Company's computers is prohibited. Vandalism of the Company's computer network constitutes a potential gross misconduct offence and could result in the learner being removed from their learning programme or apprenticeship.

The internet

It is an inappropriate use of e-mail and the Internet for learners to access or download material that can be considered obscene, offensive, abusive, sexual, sexist, religion related, racist, or defamatory. Such material can also be contained in jokes sent by email. If users receive material with such content, the material should be promptly disposed of. Such misuse of the system will be treated extremely seriously. Logging on to sexually explicit websites or the downloading and/or circulation of pornography constitute gross misconduct offences. Any form of cyber bulling or virtual bullying whereby harmful or cruel text or images is sent or posted using the internet or other digital communication whether it is intentionally/unintentionally aimed at a learner or brings the Company into disrepute is also prohibited.

Functional Skills UK (FSUK) actively monitors Internet use for content, and the amount it is used by individuals via random system checks and authorised investigations. All visited websites are clearly logged as well as times of access. Excessive private use of the Internet may lead to disciplinary action. If any material is viewed in error that does not meet our acceptable use policy, a member of the IT Services department should be informed. Failure to do this may result in later disciplinary action.

Copyright applies to all text, pictures, video, and sound, including those achieved by email or the Internet. Music and video files such as MP3s and MPEG4s which are not free to distribute must not be downloaded or stored on any part of the FSUK laptops or PC's.

Uploading material to the Internet for use other than course or work-related activities is prohibited.

Learners must never involve themselves in political discussions through outside newsgroups using the FSUK network.

The Internet must be considered an unsecured medium when transmitting data. Any transactions that originate from FSUK are carried out entirely at the user's risk. FSUK is not responsible for any on-line fraud that may occur from personal use; or the loss, damage or misuse of data.

Chat rooms

Chat rooms including Yahoo messenger, AOL Instant Messenger, MSN, ICQ etc. are not permitted unless as part of the delivered curriculum.

Students accessing social networking sites outside of learning should not, in the interests of safeguarding, include current FSUK staff as "friends". Private messages should never be sent to any staff.

Passwords

Each user is responsible for safeguarding their system passwords. Individual passwords should never be printed, stored online or given to other people. Also, user password rights do not imply that user has complete privacy. Use good practice when selecting passwords, a combination of numbers and letters is recommended for security. Do not use obvious words or phrases; try to pick hard to guess random passwords.

Computer viruses

The Company's computer network makes it vulnerable to viruses. Therefore, only duly authorised personnel have the authority to load program software onto the network system. Data compatible with the Company's system may be loaded only after being checked for viruses by authorised personnel. Any learner found to be contravening this may face disciplinary action.

If learners need assistance with any matters relating to staying safe online please contact our e-safety officer – Charlie Dew 01273 434400 or 07764 969286 or email charlie@swimuk.org. Information is also available on our website www.swimuk.co.uk in the Hub section.

Top Ten tips for staying safe online

1) Don't post any personal information online – like your address, email address or mobile number.
2) Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore.
3) Keep your privacy settings as high as possible
4) Never give out your passwords
5) Don't befriend people you don't know
6) Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do
7) Remember that not everyone online is who they say they are
8) Think carefully about what you say before you post something online
9) Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude
10) If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately.

Signed: Paul Smith

Name of employee: Paul Smith MD

Date: December 2020

Review Date: December 2021