Working Safely Online

This document provides a summary of the key principles of working safely online.

Avoid sharing or exchanging any personal information while using the internet and/or Virtual Learning Environments (VLE)
The use of chat rooms and live messaging may be part of the course delivery. These will be monitored by tutors. It is important that you only use these to post appropriate content that is relevant to the course. You should reject any unwanted requests for contact from learners outside of the class environment. Block friend/access requests from anyone you don't know.
Secure passwords are important. They should be something that others can't guess. Secure passwords include numbers, and symbols, upper and lowercase characters. Don't use the same password for every site and change them regularly. Never tell anyone your password.
When using CW&C computers and throughout your course, you must not attempt to access, download or upload on the Internet, information that is obscene, sexually explicit, racist or defamatory, incites or depicts violence, accessed to cause distress to others or describes techniques for criminal or terrorist acts.
Images, music, videos, and screensavers from the internet often have a copyright attached. Don't copy or use these files unless you have the creator's permission and you are confident it won't infringe the copyright.
Offensive or abusive language will not be tolerated during online teaching sessions, in group messages or online chats
At the end of your session make sure you log out of the programmes and computer. This will avoid other users accessing your desktop and private data.
During online learning sessions you must **not make any recordings or screen shots**. If you would like to capture some content, please tell the tutor who will arrange this.
When online it is good practice to blur your screen background. This will minimise distraction and increase your privacy. If you need help, your tutor will show you how to do this.
Throughout your course, you must not post anything online that contains: - Any offensive, obscene, harmful, threatening, abusive, harassing, slanderous, hate inciting, racist or criminal content.   - Anything that causes embarrassment to Cheshire West and Chester Council, its customers, clients, or members.   - Personal data about another person including names, contact details and sensitive personal data e.g. about another user's mental or physical health, racial or ethnic origin, religious or other beliefs.   - Messages will show who has posted them and learners must not pass messages off as being from another person.

For full details about online safety please read the Online Safety Policy and the Cyber Bullying Policy documents.

June 2021