LEARNING ON-LINE

Welcome to the Hive on- line learning

We hope that joining our on-line learning community will be an enjoyable experience for you. You will be taking part in your lessons on line and completing your assessments on line. Most of our tutors will be using Microsoft Teams for the delivery of training. Training will be a mixture of some pre-recorded resources and live sessions. Tutors are also available for further one to one support following your on-line session.

Your on-line training will take place at least once a week These training session are held as a group discussion with other learners on your learning cohort and can last where appropriate for up to two hours. If you cannot attend or need to leave early, please inform your trainer/assessor either by email, or at the start of this session.

Please find below information on using the audio, webcam and chat facilities whilst taking part in the training.

Audio
You are expected to have your microphones on mute during the training sessions at all times unless asked otherwise. There will be opportunities to ask questions during the training session. It is therefore recommended that you join the facility with the microphone and camera switched to 'off'. This function can be found on the main screen before entering the chat room.

If you are using a webcam or microphone at home, ensure you tell who is present at home that you are doing so. You don't want anything said that is inappropriate or private which is then overheard by those who are listening online in the meeting. Also, it is very disrupting to anyone attempting to present/speak and for others listening in, to hear others chatting in the background. Turning your microphone on mute can therefore avoid this.

Using Chat
If there is a message facility for texting on an online presenting program such as Microsoft Teams, be aware of sending inappropriate messages. These can be read by administrators as well as other learners and you can face action if this is deemed harassment. If you receive any messages you deem inappropriate for a chat messenger, ensure you tell the presenter/administrator immediately.

If you feel uneasy about asking questions or sending messages during the online support session, guidance is given in the videos and at the start of the online support session as to how you can contact your trainers/assessors directly to ask questions privately.

Using Webcam
If you are using a webcam for online training, ensure you check what is behind you before going live. Could it be deemed offensive? Are there people there that may not want to be filmed? If you have the facility, use 'blur background' or have a blank wall behind you if you can. Always ensure you are wearing appropriate clothing if you are using a webcam.

If the facility to ask a question only exists via a webcam, you are encouraged to switch the video to 'off' and use the microphone only, or to place something over the camera such as a piece of masking tape to avoid being seen.

Online Safety Tips.

Being safe from hackers

Everyone is a potential target. Don't think it will never happen to me. Everyone is at risk, so keep your software up to date. Turn on automatic updates and keep your devices patched regularly. This ensures that any security holes are fixed and bugs are removed that could make you vulnerable to an online hacker or data breach. If you have the administration rights to a machine, such as your own, install an anti-virus software and turn on the firewall to reduce the risk of hackers gaining access to your machine from the outside. There are plenty of free software available for anti-virus or competitively priced commercial ones.

Choosing the right password

Practice good password management! Use strong, unique passwords and never share them with anyone else! If you are using a public computer in locations such as a library or internet café, be sure to tick the box "using a public computer" this will ensure that your passwords and usernames are not saved onto the machine and cannot be remembered.

Logging off your machine

Ensure that you fully log off the machine, or fully log out/sign out of any programs you are using such as Facebook, e-assessor, YouTube and delete out the user name if it is still displayed in the login box, if the machine cannot be logged out of. This way, you won't have people logging onto your account when you walk away. Use a lockable screensaver if you have to walk away from the machine and ensure that you don't leave any written material with personal details left behind such as names, dates of birth, addresses, email, passwords etc.

Be aware of who is looking at your screen

Be aware of your surroundings, who can see your computer screen? Who can see what is displayed? Are you working on a confidential project? Are you internet banking or shopping? Can people see what is displayed and can they see you enter your card number or see your account number?

Using Public Wifi

Be aware of counterfeit wireless networks where fraudsters will attempt to duplicate the name of the WIFI for a library, train station, café. Public, free networks should never be used to carry out any personal online activities such as banking or shopping. If you must, ensure you use a VPN (Virtual Protected Network) which hides your identity online. There are many available and some come free but charges may apply for higher data usage.

Back up data

Back up your data regularly and set up a data back-up schedule, including using cloud for your mobile devices That way you know that you won't have lost much or any data, should your device become broken, lost or stolen

Phishing scams

Avoid being caught by phishing scams. So be careful of opening attachments and clicking links in emails. Do you trust what has been sent to you? Many online companies such as banks or power companies will never ask you to click a link within an email. They will expect you to go to their site or app. Never enter your card details into a link that you have followed from an email. It is most likely a fraudster!