Staying Safe Online

Staying Safe Online

Introduction

During the current Covid-19 situation, some of your course may be delivered on a blended learning basis. This means that some of your study may be in the classroom with the support of your tutor and some of your study will take place away from your tutor.

You may need to use the internet to research into topics as you complete your assessments. The following guidance will support you to stay safe online when using the internet

Staying Safe Online

How to protect yourself

Using computers and devices online has made conducting research easier. We also use the internet for everyday tasks such as shopping, banking, paying bills and keeping in touch. There are, however, a number of risks associated with the internet, which include identity theft, criminals stealing your personal and financial data to defraud you or empty your bank account.

There are a number of simple things which you can do in order to protect yourself against these risks. The precautions are as simple as choosing safe and secure passwords which are sufficiently complex, ensuring you have adequate antivirus/ antispyware installed and looking carefully at websites and emails to distinguish between genuine and fraudulent information.

How to protect your computer

It is essential to take sensible precautions to protect your computer from the any threats online. Effective protection will safeguard against your computer being infected with viruses and spyware that could result from your online activities. You may think tasks are completely harmless – such as searching the internet, downloading, playing games, and even using email, but you could inadvertently download a virus or spyware without knowing. Using anti-virus software will safeguard you against potentially serious consequences such as fraud and identity theft.

Using Smart phones and tablets

Smartphones and tablets have overtaken computers in popularity because we can access the information we need anyway, anytime. With mobile internet, email, social networking and cloud storage, you can carry out most of the tasks that you can on a computer, but in a café, out shopping, in the park or anywhere outside the house.

However, this convenience is accompanied by additional risk. Mobile devices are so small and portable, they are easier to lose or steal, leading to potential breaches to your personal and financial security. Always have a keylock or password to unlock your phone and never leave it unattended. You can set your device to remotely wipe data if it is misplaced or stolen. Some also allow you to set up remote tracking so you can locate it

Checking for fraudulent websites or scam emails

Most reputable organisations make it as safe as possible for their customers to use their websites. But today's cybercriminals are highly skilled at creating fake websites and persuading you to do what they want.

Fake websites – criminals have become adept at copying legitimate banking websites to trick customers into providing their login information. Money is then stolen from their account. It is important to carefully check the website, there should be a padlock symbol in the browser window frame, which appears when you login. The web address should begin with 'https://'. The 's' stands for secure. You can also complete checks for subtle misspellings, additional or incorrect words or characters or any other irregularities.

Phishing is where online criminals send you an email and usually there is a link to click on, to enter your personal details. They are becoming increasingly sophisticated, some examples include where fraudsters are posing as real companies, using their logo, address, and contact details. It may be a company which you may have previously contacted or done business with. You should be very wary of any email that asks for your personal details.

Another common criminal act is selling something online that doesn't exist – this scam happens so often that there is a Banking Protocol system, which alerts police to unusual activity. For example, in 2017, a retiree went to his bank to withdraw £10,000 to buy a Rolls-Royce from an advert he'd seen online. He was going to travel across the country to meet the seller and pass the money over, but bank staff thought the situation sounded unusual and contacted police through the Banking Protocol system. Police investigated and found that the car was registered to someone hundreds of miles away from the supposed seller and that it was probable

the buyer would have been robbed when he arrived to buy the car.

Fake text messages are also common, criminals send people a message via text or WhatsApp telling them there has been suspicious activity on their account and they must reply with their account number and PIN code.

Under the Fraud Act 2006, the maximum sentence is 10 years' imprisonment. Fines of between £20,000 and £100,000 are also possible.

The importance of asking 'who, what and when' when interacting with others or information online

In 2017, the term 'fake news' became part of everyday usage, and it demonstrates why it is essential to always ask specific questions when interacting with others online or when dealing with information online.

The essential questions to ask are 'who?', 'what?' and 'when?'

Who?	Do you know the identity of the person you are interacting with? Is there any way of validating that they are who they say they are? As it is rare to meet people in person who you meet online and because speaking on the phone has been replaced by messaging, it can be very difficult to know if someone really is who they say they are. An example of this is catfishing, in which someone pretends to be someone else online, e.g. an adult man pretending to be a 15-year-old boy, or a woman pretending to be a man. Catfishing has become a real issue and is possible because it is so easy to create fake profiles online. In many cases, a legitimate person's social media profile, including photographs and friends, is stolen. It is important that individuals exercise extreme caution when sharing sensitive information with someone they don't know. As incidences of sexting and gas lighting – when an individual is encouraged by someone online to share indecent images and is then bribed to prevent those images being shared – increase, it is best to always refrain from sharing images or information with someone you don't know. Asking 'who?' in online interactions will help individuals to figure out whether or not the person they are dealing with is trustworthy. It may also prevent them from over-sharing, an act which can destroy lives.

What?	What are the person's intentions? What could they get from the interactions they are having with an individual? Are they trying to get money, images or personal information from them? If the answer is yes to any of these things, then the individual should feel confident in walking away from the interaction.
When?	The times an individual makes contact may indicate something about their identity. For example, if the person only gets in contact at 2am, that may be cause for concern. Ultimately, it is important to trust your gut when interacting with others online. If the timing of the communication doesn't match with the other person's supposed work schedule, that may be a red flag.

The Internet has provided easy access to vast amounts of information on almost every subject. The difficulty is that anyone can upload information online, and figuring out what is valuable and, importantly, accurate is getting more and more difficult. By asking 'who, what and when?' you should be able to discern between good and bad information.

Who?	With such a large amount of information available, it can often be very difficult to weed out what is true from what is not. However, if you ask some of the following questions when assessing the accuracy of a piece of information, it may help you to sort out good information from bad: ● Who created it? For example, is it from the blog of an unknown commentator or from a large news outlet? ● Is it from a credible source, i.e. a news outlet or industry specialist? ● Can it be found in more than one location? ● If you type the main element of the information into a search engine, can you find the same information from other sources?
What?	What, if anything, will the writer or creator of the information gain from publishing it? For example, if a company that makes windows 'sponsors' an article about the value of replacing your windows with a specific brand (their own), then this information must be read with the understanding that it is not objective. The information has been created to entice potential customers to buy a specific brand of window. This concept can be applied to all information, but it doesn't mean that no information has any value, because even news outlets that should report facts as they are will apply personal, cultural and political bias. Rather, it means that information must be looked at objectively and valued based on the reasons behind its creation and how useful it is to you.

When?	When was the information created? The world is in a constant state of flux, which means that information that was believed to be 100% accurate a week ago may no longer be so. It is important to check and see if the infor-mation you are reading is the most up-to-date or if it has been replaced. If you have made an assumption or a decision based on old information, there may be unfore-seen consequences.

Keeping children and young people safe online

You may be a parent or a carer responsible for children's safety. We all want children to be safe and grow up happy and healthy. We must protect them from dangers including those online.

Depending on the age of the child, they may have already starting using computers, devices or social media networks. They may already be experts who know their way around the internet, apps, games, downloading and social networking with ease. They may know more about these things than you do. But they are unlikely to have the life-experience to handle all of the situations they encounter.

A few years ago, most homes had one family computer, on which parents could monitor their children to the internet, keep an eye on what they were doing and introduce a degree of control using parental software. When children started to get their own devices, it became more difficult to work with them to ensure they were visiting appropriate websites and not talking to strangers online.

Now, of course, in the age of smartphones and tablets, most parents find it a real challenge to not only educate their children in doing the right thing but control their online behaviour.

Some of these potential issues are as follows:

- Inappropriate contact from people who may wish to abuse, exploit or bully them
- Inappropriate conduct because of their own and others' online behaviour, such as the personal information they make public, for example on social networking sites
- Unfortunately, children can also become cyberbullies, especially when encouraged by others
- Inappropriate content, being able to access or being sexually explicit, racist, violent, extremist or other harmful material, either through choice or in error
- being the targets of aggressive advertising and marketing messages
- Gaining access to your personal information stored on your computer, mobile device or games console, and passing it on to others
- Using your financial details such as payment card information
- Enabling viruses and spyware by careless or misinformed use of their device

Cyber bullying

Cyberbullying can have a severe impact on the victim. It may lead to mental health problems such as depression or anxiety. It may make them wary and mistrustful or others and may find social relationships difficult. Cyberbullying can take many forms, which could include:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- trolling – the sending of menacing or upsetting messages on social networks, chat rooms or online games
- exclusion from friendship groups
- shaming someone online
- setting up hate sites or groups about a particular person
- encouraging people to self-harm
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations

If you experience any of these issues it is important to ask for help. It can be helpful to take a digital break, take time out and relax. You can report online bullying on social media and online gaming sites. You can also report it to the police as a hate crime. Please see our safeguarding contact information at the end of this book.

Digital footprint

Everything you post online stays around for a long time. Before you post anything online, use the acronym THINK. This stands for:

- **T** - Is it True?
- **H** - Is it Helpful?
- **I** - Is it Inspiring?
- **N** - Is it Necessary?
- **K** - Is it Kind?

Online radicalisation and Prevent

Radicalisation by extremist groups or individuals can be carried out via a number of ways, face-to-face by peers, in organised groups in the community and, increasingly, online. The individuals who are targeted are sometimes those who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

The internet can be used to create initial interest, and as reinforcement to other means of communication via social media. As is the case with everything it is used for, the internet enables much larger numbers of people to be reached, in a wider geographic area, and with less effort.

Social media can be used for grooming – be it Facebook, Twitter, Instagram, Tic Toc or any other sites and apps. Other online channels include chatrooms, forums, instant messages and texts. All are also used by extremists for their day-to-day communication, as is the dark web. Social media is also used for research by extremists, making it easy for them to identify a target from what they reveal in their profiles, posts/tweets, photos and friend lists.

If you are approached or groomed, think carefully about the consequences of radicalisation to yourself, your family and friends.

Everyone is subject to moods and can be affected by things that happen in everyday life. This includes being happy when something good happens or feeling anxious and depressed when dealing with a difficult situation.

Not everyone is able to communicate their feelings about what is happening in their life, but there are signs and behavioural changes that you can look out for that may indicate that someone requires help or support.

Keep an eye on family members, friends and others you think may be susceptible to radicalisation. Have their behaviour patterns changed? Have they become withdrawn for no apparent reason? Has their belief structure altered? Are they making unusual travel plans?

The Prevent duty is the government strategy to stop people from being radicalised and becoming terrorists or supporting terrorism. It places a duty on education providers and other organisations to have due regard to the need to prevent people from being drawn into terrorism. We have a clear approach to implementing the Prevent duty and to keeping our learners safe.

Please refer to Learning Curve Group Policies if you have any concerns:

https://www.learningcurvegroup.co.uk/key-policies

If you want guidance or have any questions on the content of this update email our designated Safeguarding and Prevent team **dspo@learningcurvegroup.co.uk**

If you wish to make a referral, you can contact **keeplearnerssafe@learningcurvegroup.co.uk** or call 01388777129

You can also download the Learning Curve Group Safeguarding app to report a concern and access additional information.

Websites to support you

ThinkUKnow website **www.thinkuknow.co.uk**

Get Safe online website **www.getsafeonline.org**

UK Safer Internet Centre website **https://www.saferinternet.org.uk/**

Child Exploitation & Online Protection Centre website **https://www.ceop.police.uk/safety-centre/**

Educate against hate **https://educateagainsthate.com/**

NSPCC **www.nspcc.org.uk**

Victim Support **www.victimsupport.org.uk**

Bullying UK **www.bullying.co.uk**

Internet Watch Foundation **www.iwf.org.uk**

Childline **www.childline.org.uk**

ONLINE SAFETY

Disclaimer

Every effort has been made to ensure that the information contained within this learning material is accurate and reflects current best practice. All information provided should be used as guidance only, and adapted to reflect local practices and individual working environment protocols.

All legislation is correct at the time of printing, but is liable to change (please ensure when referencing legislation that you are working from the most recent edition/amendment).

Neither Learning Curve Group (LCG); nor their authors, publishers or distributors accept any responsibility for any loss, damage or injury (whether direct, indirect, incidental or consequential) howsoever arising in connection with the use of the information in this learning material.

If you have any queries, feedback or need further information please contact:

Learning Curve Group
1-10 Dunelm Rise
Durham Gate
Spennymoor, DL16 6FS
info@learningcurvegroup.co.uk
www.learningcurvegroup.co.uk