E-safety: internet and young people

Technology, Mobile Phone



TASK 7. Assessment criteria 7. 1 & 7. 2 E-Safety is an area of growing importance and you need to be informed of the issues involved in children and young people using technology. An explanation of the risks and possible consequences for children and young people of being online and using a mobile phone. Technology is rapidly growing and offers a vast amount of benefits for children and young people. This ever growing development however also poses risks for children and young people and they need to know how to protect themselves. The various risks of mobile phones and being online can be; exposure to inappropriate content, cyber bullying, grooming for paedophiles, disclosure of personal information, piracy or illegal downloads and viruses or hacking. - Exposure to inappropriate content- This could include images that are pornographic or even images of children in a sexual nature. If children or young people view such contents it is important that they are encouraged to talk to someone they trust about this and that they are made aware of the ways in which they can be protected from such content. Parental controls help to minimise any inappropriate content being displayed but it is still not 100% safe and any content that shows harmful images of children should be reported to the internet watch foundation that monitor all contents on the internet. - Cyber bullying- This can be done using social network sites and texts and can be done anonymously and in front of a large audience. It is important to make children and young people aware of the different forms of cyber bullying and to encourage them to save any evidence of bullying received. It is also important to help children and young people understand that even if it is done on-line or via text it is still bullying and is unacceptable. - Grooming/paedophiles- Used by people with a sexual

interest in children to attempt to engage them in sexual acts either over the internet or in person. The adult attempts to make contact with children over the internet; this may be in social networking sites, chatrooms or games. This is done by pretending to be someone else, or showing an interest in them. Children and young people need to be made aware of the threats around, and encouraged to talk to adults that they trust and not to do anything that makes them uncomfortable in real life or online. - Disclosure of personal information- Social networking sites and chat rooms are based on users creating profiles including their personal opinions and in most cases their photographs. The problem with posting personal information to the internet is that as soon as it goes online, you have lost control over who will see it and how it will be used. Pictures can easily be copied and displayed in a completely different context. Because of the digital nature of the photos, they can even be altered or distorted. Children and young people need to be educated on how to keep their personal information safe so that it is not divulged to anyone. - Piracy and illegal downloads- Illegal use or duplication of material covered by laws, such as copyright. It is important to explain to children and young people that piracy or illegal downloads are the same as stealing and set out boundaries for them. There is also ways in which you can limit the sites that children and young people can visit. - Viruses and hacking- This is a very common threat to all technologies and it is needed to be understood by children and young people the importance of protecting their personal information such as passwords, home address, bank details etc and also the need to protect your system from damages through viruses. Adults can reduce the risk of children and young people being subjected to

the above threats by limiting the amount of time spent using the internet, restricting access to websites, applying parental controls, being available for the child to approach you with any problems, making them aware of the dangers and helping them gain the skills to be able to recognise the dangers. There are many websites that are also available for children and young people to become educated on how to stay safe online. A description of ways of reducing risk to children and young people from social networking, internet use, buying online and using a mobile phone. - Social networking. Talk to the child or young person about predators and about not talking to strangers or agreeing to meet them and also making them aware that many adults pose as young people to lure in children and not to be intimidated into doing anything they feel uncomfortable with online or in real life. As the adult you can use control systems that are built into some systems or download it free from sites such as Windows Live Family Safety Settings. Restrict access to social networking sites. Most social networking sites have age limits so make sure they adhere to this. As children become older help them to find sites that are well-monitored and are especially for children. Monitor the social network sites that they visit and the content of the conversations that are taking place and also take an interest in what the child is doing on the social networking website. - Internet use. Apply parental control to filter out sexual images. Monitor children's online activity and block site's that are inappropriate and limit the amount of time the child/young person spends online. Block their ability to send out personal information, use browsers that are specially designed for child/young people. Talk to children/young adults about not trusting others, not to meet people in

person and not to give out personal information (names, numbers, address, e-mail, photos or school information). Tell them to log out if uncomfortable about anything. Encourage the children/young people to be aware of the risks of the internet. You should encourage children and young people to talk to you about things that might be happening on-line and guide them in the right direction. This will help them to recognise the dangers that could develop. Placing the computer in a main room where you can supervise the use and support them whilst they are using the computer on-line will help minimise the risks. - The Byron review was published in 2008 which has stated in order to minimise the risks for children and young people, that parents will hold the key role. Video games must now be clearly labelled with age ratings (from 3 years to adult, a logo on the back of the game to represent each age group) and computers sold for home use should be kitemarked with parental control measures (software). They also set up an awareness campaign on child internet services and behaviour and advised that schools should have an acceptable use policy in place that Ofsted will monitor. - Buying online. There is a risk of others hacking into your computer to get your identity this can be minimised by a firewall. A firewall can help by preventing hackers or malicious software from gaining access to your information. There is a risk to young persons of fraud whilst buying online. This can be prevented by using a secure payment system (PayPal), which enables you to buy from multi online shops and pay using one account set up by PayPal. The account is set up and verified by PayPal who take two small payments from your debit card to verify that you are who you say you are, then you can use the account via a password system. - Using a mobile

phone. There is a risk to their health by means of cancer/tumour which can be reduced by using landline phones, hands free, loud speakers or blue tooth. Using less time on phone calls by perhaps the use of text messages instead can also make a difference. There is also a risk of the child or young person being attacked if they have expensive phones so a cheap pay as you go phone for them to use will minimise the risk and still allow the child/young person to have access to a phone.