Keeping Myself eSafe

Information for Teachers

Communication Technology

Communication Technology

One of the most significant outcomes of the digital age has been the evolution of communication technologies.

When young people use computers at home, they can be communicating with friends in many different ways, such as social networking and instant messaging websites, and mobile phones and hand-held devices mean that they can always have access to the internet.

Communication technology offers huge benefits and opportunities. Not only does it help young people develop their communication skills, it also allows them to contribute to online communities in creative and meaningful ways.

Communicating with the outside world, however, poses threats to the safety of young people. It is important that they understand the potential risks and the e-safety strategies that can help them stay safe online.

The main areas of communication technology covered in the section of the Guide are:

- Instant messaging
- Internet chatrooms
- Email

Note: Social networking technologies such as Bebo, Facebook and MySpace are covered in another section of this Guide.

Instant messaging

In its simplest form, instant messaging (IM) is an online technology that enables users to communicate with others in real time ie, when you send an instant message, it is immediately viewed by the other person, unlike other technologies, such as e-mail, where there can be a delay.

IM is an easy way of sending a written message to a friend, or to a group of friends, who are online at the same time. The instantaneous nature of IM means that young people frequently use it to chat, or have 'conversations' online, no matter where they are in the world. IM has become part of their everyday lives and is an important ways of staying 'wired' to their friends.

In addition to text messaging, IM technology also supports voice chat, group chat, webcams and file exchange. IM can be accessed through computers, mobile phones and some hand-held devices such as iPods.

Some of the most popular IM services include:

- MSN Messenger
- Google talk
- ICQ
- Yahoo Messenger
- AOL Instant Messenger

To use a programme such as MSN Messenger, software must be installed on the computer. This registration process usually requires the user to provide personal information such as their name, email address, age, gender and location. This information may be transferred automatically to a 'member directory' or 'public profile', which can be viewed by other users, and is sometimes shared with chat systems.

The user creates a 'buddy list' ie, a list of contacts with whom they might wish to exchange messages. This means that the user is alerted when their 'buddies' are online, and vice versa.

Communication Technology

Risks

Any interactive area of the web which is used by children inevitably becomes a target for sexual predators, and this is a significant risk to young people. Sexual predators have realised that instant messaging is a way of:

- making initial contact with children from member directories or profiles
- gathering personal information about children so that they gain their confidence
- communicating with children in a direct and instantaneous way
- always knowing when any particular child is online
- grooming children with a view to isolating and manipulating them
- operating in an environment of relative anonymity

A sexual predator's aim is to isolate a child and progress their communication into a private domain, such as a mobile phone, and then ultimately to sexual contact.

There are other risks associated with instant messaging:

- some users may make inappropriate material available via file transfer or live webcam images
- pornographic website operators sometimes create fake profiles containing links to their sites, and send messages with such links to other users
- files or links accessed from messages in chat rooms may carry viruses, and dialer programmes linked to high cost telephone services
- instant messaging has become one of the main forums for bullying behaviour (see section on Cyberbullying)
- communication technologies can be a forum for arguments and abusive exchanges, a phenomenon sometimes referred to as 'cyber wars' or 'flame wars'.

Young people using these need to be aware of the risks and encouraged not to give out personal information that may identify them and place them at risk.

Internet chat rooms

Internet chat rooms are places where people go to have conversations and discussions online. Users contribute to chat rooms (sometimes known as internet forums) by posting a comment or message, sometimes in response to someone else's post, and the ensuing conversations are known as 'threads'.

These forums are often dedicated to common interest topics or themes such as music, football or television programmes. Everything that is posted can be seen more or less instantaneously by everyone else using the chat room.

Chat rooms can be a lot of fun and they have an element of anonymity, so young people often talk about things they may not have the confidence to say face to face. They can pretend to be someone else, perhaps older and more popular.

It is the anonymity surrounding internet chat rooms, however, that poses the greatest risk to young people because they do not know who they are chatting with. Because of this - and because chat rooms are particularly popular with young people - there is a risk that they can be used by paedophiles or sexual predators searching for victims.

Adults who want to exploit children might pose as young people themselves, attempting to create the emotional bonds and friendships that form the basis of grooming techniques.

Risks

Sexual predators recognise that chat rooms are a way of:

- making initial contact with children
- using common interests such as music and games as a means of gaining their confidence and building trust
- gathering personal information about children
- grooming children with a view to isolating and manipulating them
- operating in an environment of anonymity

Online grooming

Grooming is when a person tries to 'prepare' another person to be the victim of sexual abuse.

Although not all sexual abuse begins with grooming, it is a very common process which involves the groomer spending time building a trusting relationship with a child before the abuse takes place. Victims of grooming often do not realise that they are being manipulated until after they have been sexually abused and, even then, some victims do not make the connection between grooming and abuse.

Online grooming usually involves a predator setting up an abusive situation using technologies such as instant messaging, social networking websites, internet chat rooms and mobile phones. It is very common for sexual predators to source victims on the internet by posing as a child.

Groomers try to find out as much as possible about their potential victims, for example:

- their age
- what they look like
- mobile phone number
- when they are at home
- how they feel about themselves

The way that young people use communication technologies such as IM and social networking websites, means that much of this information is provided at registration or when creating personal profiles. Young people must, therefore, be aware of the risks involved when divulging personal information.

Establishing an online 'relationship'

In most cases a groomer wants to be seen as a trusted and respected peer, or as a caring and understanding person who shows empathy to the victim. Being in this trusting relationship with the groomer makes the victim less suspicious of their actions and intentions. That's why it is often confusing for the victim when the abuser begins to do things that make them feel uncomfortable.

Grooming techniques

After a trusting relationship has been established, groomers use various techniques to prepare their victims. These include:

- talking about sex in a way that is inappropriate for the child's age and stage
- enquiring about a child's physical and sexual development
- sharing their personal problems with the child

A sexual predator's aim is usually to isolate the child and progress the conversation into a private domain, such as on a mobile phone, and then ultimately to sexual contact.

Exposure to sexual material

Groomers often expose their victims to inappropriate and illegal sexual materials. These might include pornographic images and videos, drawings and animations, text messages, stories, sound bites and music. Some of this material will be illegal to show or sell to those under a certain age.

Viewing such materials can be very upsetting and traumatising for young people. Although exposure to such materials might only be part of the plan, the process itself is abusive and in some cases criminal.

Online grooming sometimes involves the victim engaging in sexual behaviour at the request of the groomer, including sexually explicit text messages, sexually explicit images and videos via web/phone cam.

It is not uncommon for groomers to threaten to hurt or kill family members and pets if the child does not comply. The groomer might also threaten to tell the parents that the child has acted inappropriately (eg, sexually) online.

Email

Electronic mail or e-mail, is a means of writing, sending, receiving and saving messages over electronic communication systems.

Although the growth of instant messaging and mobile phone technology has provided more popular ways for young people to communicate, most have e-mail accounts at school and at home.

The main personal safety issues relating to e-mail are:

- spamming
- phishing
- malware
- flaming
- contact by sexual predators.

Spamming

Spam is unwanted email, almost always from an unfamiliar source. Because of the very low cost of sending e-mail, spammers can send millions of e-mail messages each day over an inexpensive internet connection. Although spam is inconvenient and frustrating for all users of e-mail, for young people there are additional concerns. Spam often contains inappropriate content such as advertising – possibly under the pretence of offering a prize - and children may be tempted to click links which take them to other web sites. Many Spam e-mails contain links to pornographic content or attachments that are unsuitable for children to view.

Phishing

Phishing is becoming increasingly common on social networking sites. Phishing is when a fraudster sends e-mails or IMs pretending to be the victim's bank or an online service such as Paypal. These messages are often pop-up boxes which appear genuine, and are designed to encourage users to provide bank and credit card details such as account numbers, passwords and PIN numbers. These are then used fraudulently to purchase goods, with serious financial consequences for the victim.

Although young people may not have credit cards, many have savings accounts and so they need to understand the dangers of phishing and other attempts to gather personal information. On no accounts should they respond to unsolicited emails, pop-up advertisements or unknown website addresses, even if they look official and secure.

E-mail worms and computer viruses

Malware is short for malicious software and is designed specifically to disrupt a computer system. A Trojan horse, an e-mail worm or a virus are examples of malware.

Malware commonly attaches itself to another programs or data files in order to spread and reproduce itself without the knowledge of the user. Some are annoying (for example pop-up slogans) but cause no significant damage. Others, however, can be harmful by destroying data or corrupting disks.

Because viruses are designed to be concealed in legitimate programs or data files, they usually spread from computer to computer by people who are unaware that they are doing so.

Typically, viruses are transmitted via:

- Attachments to e-mail messages
- Downloading or sharing files from the internet
- Clicking internet links that activate malware
- Using infected disks or memory sticks

Sophisticated and damaging viruses are becoming more and more widespread, and unless anti-virus software is installed on a computer, there is no sure way of knowing whether there is a virus within the system.

In recent years, there has been a growth in increasingly sophisticated malware that is designed to discover and relay private information stored on a computer. Such programs are usually referred to as 'data mining' software and they can seriously compromise the security of any information stored on the computer, in particular passwords, financial data such as bank details, and personal details about individuals which can lead to online fraud and identity theft.

Young people must be aware of the risks and potential consequences associated with malware, and of ways in which private information can be protected.

Flaming

The ease and impersonal nature of modern email and instant messaging means that they sometimes give rise to what is referred to as flaming.

Flaming occurs when one person sends an angry or antagonistic message, which can easily escalate into arguments and abusive exchanges – a phenomenon known as 'flame wars' or 'cyber wars'.

Flaming is assumed to be more common today because, unlike face-to-face contact, typing a message to another person is an indirect interaction, so civility may be forgotten.

It's easy for young people to forget that such behaviour can cause upset and distress for the recipients and, because abusive or threatening messages may be saved and printed, senders may be held accountable for their actions.

Contact by sexual predators

E-mail is less anonymous than other communication technologies such as instant messaging and internet chat rooms, and therefore less attractive to sexual predators as a way of contacting children.

Many young people, however, use free webmail accounts and, because some internet service providers allow email addresses to be shared with third parties, this can result in contact details and other information about children reaching a wider audience.

When young people use email, they are always at risk of receiving unsuitable messages or being contacted by sexual predators. They must therefore know the appropriate behaviours and safety strategies to adopt in these circumstances.

Safety Strategies

1) When you register for a service such as IM, e-mail or an internet chat room, only provide information that you are happy to provide.
2) Never give out your personal details to anyone on the internet. This includes your messenger ID, email address, home address, mobile number and any pictures of you, your family or friends.
3) If you must give personal details, keep a record of what information you gave, to whom and when.
4) Make sure you know everyone on your 'friends' or 'buddy list'. If you haven't met people face-to-face, they may not be who they pretend to be. Think carefully before answering emails or instant messages from people you don't know.
5) Make sure you know how to block instant messaging contacts. The sender will not be told you have blocked them; you will just appear offline in their contacts list, so they cannot message you. Don't forget you can always delete a contact if you don't wish to talk to them anymore.
6) If you have your own profile on IM, it's not a good idea to have a picture of yourself. You can use one of the pictures that are on IM already, or a picture of a cartoon character.
7) Never agree to meet strangers offline.
8) Remember the importance of good manners and 'netiquette'. Never post abusive or hurtful comments about anyone and avoid getting involved in online arguments where you say things that you might later regret.
9) If someone upsets you online, walk away from the computer - that way no one will get hurt. Take five minutes to do something you enjoy doing to help you calm down, then reply with a clear head.
10) If you feel someone is being strange with you or your friends, or if someone is bullying you on a networking site, contact the administrator of the chat area or tell a trusted adult.
11) If you receive a message that is either harassing, of a sexual nature, or threatening, tell a trusted adult. You can forward a copy of the message to your Internet Service Provider and ask for advice or assistance.
12) Learn to recognise spam or junk email and phishing scams. Don't believe them, reply to them or use them. Never click links in email messages.
13) Never download files or content from people or sites that you aren't sure about. Even if the file comes from a friend, you must still be sure what the file is before opening it.
14) Make sure that your computer has up to date anti-virus and anti-spy software installed.