Keeping Myself eSafe

Information for Teachers

Social Networking

Social Networking

About Social Networking

Of all the facilities offered by the internet, online social networking websites have become the most significant in the day-to-day lives of young people.

Sites such as Bebo, MySpace and Facebook, have become increasingly popular in recent years, and the number of registered users has grown rapidly. Bebo, for example, has more than 8 million users in the UK, and almost 70% of all 13-17 year-olds in Britain have profiles on networking websites. It is quite normal for young people to have profiles on more than one site.

Staying connected

For young people, online networking is the cyber equivalent of hanging out with friends – a space in which they can chat, post messages and share things. Unlike other forms of communication such as the telephone, networking sites make it possible for young people to be connected to lots of friends at the same time. This has led to the rapid growth of online 'communities', where friendship groups use social software to stay connected and to develop new friendships.

Social networking services are websites with a range of tools that enable users to:

- Communicate with others and develop new friendships or contacts
- Represent themselves online, often through the creation of a personal profile
- View content and find information
- Create and upload content, such as images, music and videos
- Share third-party content including images, music and videos
- Post messages – both public and private
- Collaborate with others, eg planning events

Social Networking

The most popular social networking services are organised around the profiles of members. When young people sign up and create their own profile, they are encouraged to provide standard information about themselves, eg:

- About me
- My physical appearance
- Where I live and go to school
- My likes and dislikes
- My favourite music, films and games
- Favourite sports
- The person I'd like to meet
- I'm happiest when …

Online identity

Young people spend a lot of time creating and customising these online identities, since their profile projects the way they want to be perceived by the outside world. Many decorate their profiles with patterns and colours (usually called 'skins'), photographs, graphics, sounds, and music to match their personality and interests. There is often an option to upload personally recorded videos, as well as those uploaded from other sites such as YouTube.

Some sites allow users to maintain their own Blogs (web logs) where they can record thoughts or write about events in their lives. It is like a diary, but is designed to be read by other people. The increased affordability of digital cameras and editing software has enabled people to record and publish videoblogs.

Users can also take part in discussion groups and special interest chatrooms.

The user's profile page enables them to create lists of 'friends' ie people they communicate with regularly and in most cases their real life friends. Depending on the level of privacy set by the user, it may be possible for other people view the profile and leave comments and the user can decide whether they'd like to add that person as an online friend. Most sites provide a link to a page which lists all of the user's friends.

In summary, social networking allows young people to publish information about themselves online, visit each other's profile and leave comments, send and receive messages, publish (upload) and share photographs, music and videos, maintain current friendships and create new contacts.

Risks

The main reason for the huge growth in social networking sites is that they offer young people many different ways to communicate. Unfortunately, this also creates opportunities for people to use social networking for mischievous, harmful and illegal purposes. These include:

- Bullying, intimidation and harassment
- Grooming by online sexual predators
- Fraud and identity theft
- Publication of unsuitable content, including pornography, hate, racist and self-harm materials
- The promotion or glamorisation of anti-social behaviour such as drinking, drugs, fast driving and violence
- Breaking the law by publishing copyrighted material online

Research suggests that many young people have a casual attitude to e-safety when it comes to social networking. A recent survey of teenagers found that a significant number made little effort to protect personal information and regularly accepted strangers as online 'friends'.

- The majority of teenagers made no effort to hide their personal information online
- The majority of teenagers had accepted strangers as online 'friends'
- Half of the teenagers had witnessed cyber-bullying
- 70 per cent left their profiles public, meaning anyone could access their information or copy their images
- Only 18 per cent limited their profile information to 'friends'
- 13 per cent did not know how to restrict access to their information
- 12 per cent posted their mobile phone number online
- 25 per cent had accepted 'loads' of strangers as 'friends' online
- One-third said it was very easy to access adult material online

Source: National Centre for Technology in Education; Irish Times, 7 February 2007.

Social Networking

A public space

Perhaps the main risk in social networking is that young people believe that they are publishing information for a closed group of friends. Many are unaware that the information they have posted may be publicly available and read by a much wider audience.

For example it may not occur to young people that comments they make about teachers or inappropriate photographs of themselves, may be accessed by others and used in ways that can cause harm and distress. Once these are uploaded to a profile, young people run the risk of losing control over them.

Netiquette

Sometimes, young people forget the importance of good manners and behaviour online.

Differences of opinion between people can quickly escalate into arguments and abusive exchanges, a phenomenon sometimes referred to as ‘cyber wars’ or ‘flame wars’. Networking sites can be used as a vehicle for making abusive comments about others cyberbullying and harassment.

It’s easy for young people to forget that such behaviour can cause distress for victims, and the public nature of social networking sites means that they can be identified and held accountable for their actions. (Note: Cyberbullying is covered elsewhere in this Guide.)

Netiquette is a term referring to good behavior when using internet facilities such as social networking websites, emails, newsgroups, message boards and chat rooms. Some examples of netiquette are:

- Not using someone else’s name or pretending to be them
- Not posting or distributing material that is deemed offensive or illegal
- Not using abusive or threatening language
- Not posting discriminatory remarks regarding people’s sex, race or gender
- Not spamming message boards or chat rooms with useless or repeated messages
- Not trying to obtain or use someone else’s password or other personal information

Sexual predators and online grooming

Because some young users of social networking sites take a causal attitude to privacy and security, they can be vulnerable to an approach from sexual predators. Some paedophiles are very adept at creating online identities where they pretend to be a young person. Their aim is to befriend and groom children, with the possibility of meeting them 'offline'.

Although the most popular networking sites set a minimum age for registration (for Bebo it is 13), it is difficult to enforce this. A significant number of young people are unaware of the potential risks and consequences of joining social networking sites.

Sometimes young people aren't careful about who they'll accept as 'friends' because online popularity is often measured by the number of 'friends' added to a profile. Every time a young person accepts a new 'friend', it widens the network of people with access to their profile, and increases risk of personal information falling into the wrong hands.

It is, therefore, vital that young people understand the importance of keeping their profiles private. If they don't, anyone can access their information and contact them, particularly if their profile contains their home address, mobile number, email address and school.

Photographs and images

Publishing a personal photograph or image increases the level of exposure and risk to personal safety. Photographs that seem innocent can give away identifying information such as their school or sports club. Photographs with a 'tag' can put a name to a face. (Using the 'tag' feature means a small box will appear on screen to name each person in a photograph.)

Sharing photographs is one of the most popular activities on social networking websites, but there is a growing concern about the publication of inappropriate photographs of young people. A teenager might publish an immature, rude or compromising photograph on their profile for fun without realizing that it may be viewed and downloaded.

Apart from concerns about exposure to sexual predators, children should be aware that they lose control of a photograph when it is uploaded to a social networking site. The photograph can be removed from their profile, but it can never be deleted from the internet and it might reappear later in life, causing considerable embarrassment. Many employers admit to checking the profiles of potential employees when recruiting staff.

Photographs and personal vidoes can be altered using software such as Photoshop and published on other websites or used in the cyberbullying of victims.

There is a danger that a teenager concerned with their appearance might publish a ‘sexualised’ image of themselves online. A sexualised image does not necessarily feature nudity - it can portray the young person posing in a manner that has sexual overtones. Some websites allow users to rate a photograph as ‘hot or not’. Again, such images can cause considerable embarrassment in later life.

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.

Identity theft

Social networking sites are designed in a way that encourages users to publish personal information. Because this information can easily be copied and published on another website, young people must be vigilant tnd take extreme care.

Identity theft is the theft of a person’s details which are then used, without their permission, in a fraudent or deceitful way, to obtain money or goods.

The increase of malware programs designed to ‘mine’ private information about individuals is one of the major contributors to identity theft. Malware that searches for private information such as address, bank and credit card details, PIN numbers, dates of birth, tax and employment information, and passport details, can lead to identity theft.

Protecting information

It is important that young people understand the importance of protecting personal information online. When signing up for social networking sites, they must set appropriate privacy levels and take care before publishing any person information that could be harmful if it fell into the wrong hands. They should ask themselves, “Is it necessary to reveal this piece of information about myself?”

Registration forms often contain fields which which don’t have to be completed, for example a nickname or alias can be used instead of a genuine name.

Care should be taken, however, when choosing a username. For example ‘Sex Kitten’ or ‘Boy Racer’ don’t give a positive impression, and may lead to contact from the wrong types of people.

Inappropriate content

The facility to publish and share content is one of the most attractive features of social networking sites. Young people particularly enjoy sharing music, images and videos – much of which is downloaded from third party websites such as YouTube.

Some websites warn that people who upload content containing nudity, violence or offensive material will have their accounts deleted, and moderators use special software to find and remove such items. But even so, inappropriate content does find its way online and can remain there until found and deleted.

Sexual or pornographic materials represent only one form of inappropriate content. Social networking sites have been used to promote violence, terrorism, discrimination, crime, gambling, extreme political views and cult worship, all of which may potentially be harmful to children. Sites extolling the virtues of knives and guns have become increasingly popular with some young people.

Intellectual property

Young people spend a lot of time creating and customising their profiles. This often involves uploading music, sounds, graphic images, photographs and video materials. They may be unaware of the issues associated with downloading the intellectual property of others, and then publishing (or sharing) such items on social networking sites.

It is quite common for children to download music or images from the internet and then customise them by remixing sounds or splicing together images from movies and advertisements to make their own mini-films.

It is important for young people to be aware of the implications of breeching the intellectual property rights of others, both in terms of the moral issues and the legal consequences.

Social Networking

Safety Strategies

Initial security precautions

1) When you register for a social networking site, only provide information that you are comfortable with. You don't need to complete all the fields if you don't want to.

2) Don't use your real name when setting up your account. For example you can use only your first name or a nickname. Your friends will know where to find you.

3) Be careful about the information you publish on your profile. If you wouldn't be happy about printing it off and handing it out on the street, why would you want to have it on your profile?

4) Don't post your address, phone number, email address or messenger ID on your profile. None of your friends would need this information.

5) On your account, set your privacy levels so that only approved friends can view your profile and message you. This means that people you don't want to see your profile can't.

6) Instead of publishing a photograph of yourself, consider using an avatar, or a cool graphic, or picture of your favourite band. That way, strangers won't know what you look like.

7) Select the 'No Picture Forwarding' option on the settings page – this will stop people forwarding your pictures to anyone without your consent.

8) If you do post pictures of you and your friends, make sure there are none in school uniform. The school badge can give away where you go to school.

Communicating with others

9) Make sure you know everyone on your friends list. If you haven't met the people face-to-face, they may not be who they purport to be. Think carefully before answering emails or instant messages from people you don't know. Review your list of online 'friends' regularly.

10) Be careful who you accept into your private chat areas. If you know someone… who knows someone… who knows someone, it still doesn't make them your friend, so think carefully about whether you should be chatting to them and what you're saying.

11) Unless you know your 'friends' offline in the real world, they are just cyber friends. Never trust cyber friends with important details about yourself or share personal information, no matter how tempting it may be. You never really know who you are chatting with.

12) If you write a blog, don't give too much away. It's okay to tell the world that you are having a party at your house, but don't post details of where it is or when. Your real friends can phone or message you to get details.

13) Don't fill out any 'fun' questionnaires that are sent to you, even if they are from your friends. Remember, you're in a world where everything can be forwarded without your permission.

14) Never agree to meet strangers offline.

Netiquette

15) 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. Many cyber wars start with a careless message.

16) 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.

17) Never use someone else's name or pretend to be that person.

18) Never give out personal information about your friends. Think how you would feel if someone did that to you. Don't send pictures either - posting an embarrassing picture of someone else is unfair and is a form of bullying.

19) Never post discriminatory or abusive remarks regarding people's sex, race or gender

Sharing content

20) Think carefully about what you are uploading and what might happen if it got into the wrong hands. There's no such thing as 'private' on the Internet. People can find anything they want and keep what you post – forever!

21) 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. Hacking tools and programs (such as Trojan horses) can give someone a backdoor to your computer, all your passwords and personal information.

22) Be careful about sharing pictures of yourself, especially if they are the sort that you wouldn't want your parents or teachers to see. Photographs and other images can be downloaded and used in ways that you might find embarrassing or upsetting.

23) Don't break intellectual copyright by uploading or sharing images, music or film that is the work of other people. It is against copyright law to do this. You don't have the right to alter someone else's work either.

24) Never post or share material that is offensive or illegal.

Spam, junk and phishing

25) Don’t be fooled by a phishing scheme. Never respond to email or an IM that you think is suspicious, a pop-up advertisement or a link to an unknown website address, even if they look official and secure. You can always check whether the link is real by typing it into your browser.

26) Learn to recognise spam or junk email and texts. Don’t believe them, and don’t reply to them, or use them. Never click links in junk email messages.

Reporting problems

27) If you feel someone is behaving in a strange way with you or your friends, or if you are being bullied on a networking site, contact the administrator of the chat area or tell a trusted adult. Remember that you can always block that person from contacting you again.

28) If you receive a message that is either harassing, of a sexual nature, or threatening, tell your parents or your teacher. You can forward a copy of the message to your Internet Service Provider and ask for advice or assistance.

29) If you think that the person who is contacting you may be an adult who wants to abuse you or your friends, report the issue to the site or speak to a trusted adult. The popular networking sites have tips and advice for users about staying safe and procedures for reporting suspicious behaviour.

30) Print out any messages and make sure not to delete them. The police need the original message to check out the headers and other information to trace the source.

Social Networking