BERWICK MIDDLE SCHOOL

GUIDANCE ON SAFE INTERNET USE FOR 8-13 YEAR OLDS

SOCIAL NETWORKING SITES – what are they?

Social Networking websites utilise applications, which help connect friends using a number of tools like blogs, profiles, internal email systems and photos. Well known sites include Bebo, Myspace, Facebook and LiveJournal, and these have become an influential part of contemporary culture. These types of sites allow users to be incredibly creative online, keep in touch with their friends and express themselves using a whole range of different media and applications such as video, photos, music and chat. However, it is important to realise that whilst these are fun and offer great possibilities, there are potential risks including **cyberbullying, inappropriate sexual contact and the misuse of personal information.**

Users sign up and create their own profile or 'space'. Often, these contain standard sections such as 'About Me' and 'Who I'd Like to Meet' and also include things like Music, Films, Sports, Scared Of and Happiest When. They can also add specific personal details such as physical appearance, school/workplace etc. Most sites also have a blog (see 'What is a blog?' for definition) where users can write daily thoughts or include articles, which they find interesting.

An important element in social networking is the user's ability to customise their 'space', e.g. by changing the colour of their profile, adding applications to their profiles, uploading images/ pictures onto their profile. One picture can be chosen as their "default image" which will be seen on the profile's main page. There is often also an option to upload videos including music videos/personally recorded films, once posted there is little if any control over what happens to this media. Content can be copied, altered and reposted by anyone and it's very difficult to take back what may be later regretted. This can damage reputations as well as future prospects.

What's this?

Blog

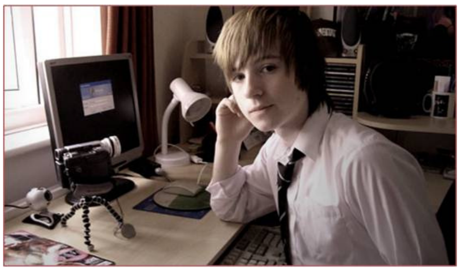
A blog is a website on which items are posted on a regular basis often focussing on a particular subject such as food, local news or politics; or as an online diary. A typical blog combines text, images, and links to other blogs, web pages, and other media related to its topic. Since its appearance in 1995, blogging has emerged as a popular means of communication, affecting public opinion and mass media around the world.

Forum

Forums are areas in which participants can leave messages, often in response to a topic. Often these messages are moderated, and the chat is not instant, as with chat rooms and instant messenger. Some social networking sites also provide users with an opportunity to create or join common interest groups, which also utilise forums. Young people often use these to share views on contentious issues and to motivate others to support their cause, making them great for debating.

Network

A network is a general group on a social networking site based around a common characteristic for instance a region, workplace, university or secondary school. If a user joins a network then they can find out more about the other users within the same network.



What are the risks?

Although chatting online can be great fun, users, in particular young people, can sometimes find themselves in situations where they can feel out of their depth control. Risks can arise when young or vulnerable people give out their personal details to strangers. For them the online world can often seem very different to the real world, and they can be tempted to say and do things that they wouldn't dream of if they met someone face to face. This can include giving out personal information such as mobile numbers and pictures of themselves.

If they are talking to another person there is a risk that they will misuse this information, for example, by texting abusive messages to the person, or by posting their image on a website; but there is obviously a greater risk if the person that they are chatting to is not who they think it is. Unfortunately, paedophiles - adults who want to meet young people for sex - use the internet, often with the intention of talking with and meeting a minor. Young people can be naive to this risk, and often feel that they are invincible, or that 'they would know if someone was lying'.

Younger, less confident people swap friends' through IM, and therefore can be chatting to strangers who they feel they trust because a friend of a friend knows them. IM is a very intimate form of communication - more so than a chat room with many participants, and therefore child abusers will often use this as a means to extract personal information from a young person.

What are the recommended age restrictions for IM and SNS?

FaceBook	13
BEBO	13
HABBO	13
MSN	No limit stated
MySpace	13
YouTube	No limit stated
Club Penguin	No limit stated
Neopets	13
Stardoll	7
PopTropica	13
Pizco via email	13 – needs parental consent
YouTube	13

None of the above sites (except Pizco) perform any checks to verify the date of birth entered is correct!

How can we protect young or vulnerable people using social networking websites?

- Encourage them only to upload appropriate pictures – if they don’t want their parents, teachers/stranger on a train to see it – they shouldn’t post it!!
- Anything too sexy to be passed round the dinner table should NOT make it on to the web. It's also not a good idea to post pictures, which can identify their school or workplace since this could help someone locate them. If photos include images of other people, make sure they ask their permission before posting the picture on the web
- Don’t let them post their phone number or email address on their homepage.
- Advise the use of privacy settings so that only approved friends can instant message them. This won't ruin their social life – new people can still send them friend requests and message them, they just won't be able to pester them via Instant Messenger (IM).
- Check if they have ticked the “no picture forwarding” option on their social networking site settings page – this will stop people sending pictures from their page around the world without their consent
- Encourage them not to give too much away in a blog. Friends can call them for the address of the latest party rather than read about it on their site. REMEMBER THE PARTY IN APRIL 2008 NEAR CHESTER LE STREET WHEN THE HOUSE WAS TRASHED
- Ask them to show you how to use a social networking site - getting involved will empower them to share the experience with you.
- If they are being harassed by another user keep the evidence and report that person’s screen name to the social network provider.
- If you think that they have been the subject of an inappropriate sexual contact or approach by another person, its vital that you help them to keep a copy of the evidence and report it to the police via the Child Exploitation and Online Protection (CEOP) website www.ceop.gov.uk/reportabuse

As a parent/carer it’s really important to familiarise yourself with social networking services.

Most sites stipulate a minimum user age of 13.

BY UNDERSTANDING THESE SITES YOU CAN HELP TO SUPPORT YOUR YOUNG PEOPLE IN CHOOSING AN APPROPRIATE SITE AND USING IT IN A SAFE AND CONSTRUCTIVE WAY.

Instant messaging – what is it?

Instant messaging (IM) is a form of real-time text-based communication conveyed over a network, such as the internet, between two or more people on a user's contact list. Examples include Windows Live Messenger, Jabber, ICQ and AIM. IM technologies often include additional features that make them even more popular such as having the ability to talk directly for free; to share files; or to view the other party through a webcam.

In instant messaging applications, a buddy list is a list of a user's contacts that they converse with through instant messaging. On such lists users can view if their contacts are online, offline, online but busy etc. Often younger young people will give share their friend lists as try to get as many friends as they can.

Users can block contacts that they no longer wish to talk to.

Instant messenger is one of the most popular ways of chatting for young people. Young people often feel that they can talk more intimately in this environment, and often use their own text style language to do so.

WHAT ARE CHAT ROOMS?

A chat room is an online forum where people can chat online (talk by broadcasting messages to people on the same forum in real time). Sometimes these venues are moderated either by limiting who is allowed to speak (not common), or by having moderation volunteers patrol the venue watching for disruptive or otherwise undesirable behaviour.

There are three main types of chat room:

- Internet Relay Chat (IRC) – the oldest and still popular form of chat room is the text-based variety. It is a real time form of synchronised internet chat.
- 2D Visual Chat Rooms provide a virtual world or graphic background that a user's avatar can navigate. These environments are capable of incorporating elements such as games and educational material most often developed by individual site owners, who have a more in depth knowledge of the system. Some visual chat rooms also incorporate audio and video communications, so that users can see and hear each other.
- 3D Visual Chat Rooms e.g. Habbo Hotel– These are very similar to the 2D variety except that they utilise 3D graphics. This allows the user a more realistic interaction with the environment. The most popular environments also allow users to create or build their own spaces.

What are the risks with Instant messaging?

Although chatting online can be great fun, young people can sometimes find themselves in situations where they can feel out of their depth. Risks can arise when young people give out their personal details to strangers. The online world can often seem very different to the real world for young people, and they can be tempted to say and do things that they wouldn't dream of if they met someone face to face. This can include giving out personal information such as mobile numbers and pictures of themselves. If they are talking to another child there is a risk that they will misuse this information - for example, by texting abusive messages to the child, or by posting their image on a website; but there is obviously a greater risk if the person that they are chatting to is an adult.

Unfortunately, paedophiles - adults who want to meet young people for sex - use the Internet, often with the intention of talking with and meeting a child. Young people can be naive to this risk, and often feel that they are invincible, or that 'they would know if someone was lying'. Young people will often 'swap friends' through IM, and therefore can be chatting to strangers who they feel they trust because a friend of a friend knows them. IM is a very intimate form of communication - more so than a chat room with many participants, and therefore child abusers will often use this as a means to extract personal information from a young person.

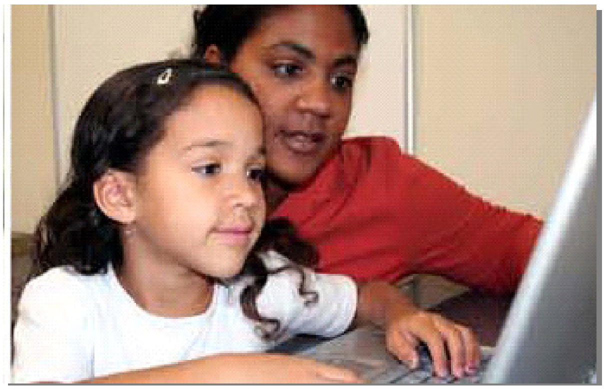
Minimising the Risk

You can minimise the risks by taking the following simple measures with your young people: It is vital that you know if your child uses chat applications online, and that you emphasise to them the importance of keeping their personal information personal.

- If your child uses IM then it is a good idea to ask them to show you how it works - in this way you can also gauge who they have on their contact list and if there is anyone how they don't know in the real world.
- It is also a good idea to ask them if they know how to block someone who they no longer wish to talk to.
- You can also direct them to the Thinkuknow website, where they can watch films and play games on how to stay safer online.
- Consider creating some family rules which you will all agree to on online use, including not giving out personal information, or talking to strangers without discussing it.
- Remind your young people that they should never meet up with someone that they have met online without you or another adult going with them.

What should I do if I am still concerned?

If you are concerned they may be at risk, it may be necessary to log or monitor their conversations, and this can be done though some forms of filtering software - but this should be considered carefully, since they may feel that they have to hide more from their parents if they think they are not trusted. GetNetWise has lists of filtering and monitoring software.



Finally, it’s really important that you encourage your child to tell you about any illegal or inappropriate activity they come across or indeed anything that makes them feel uncomfortable.

WHAT DO I LOOK LIKE? I'M A CUTE FLUFFY BUNNY..

The use of mobile phones

Young people like to use mobile phones as it increases their feeling of independence as it enables them to plan arrangements with friends and family. They can also have a lot of fun with games, ringtones and by using mobiles to take pictures. Young people can also exchange data (e.g. pictures or ringtones) wirelessly over short distances using their phone's bluetooth technology.

As mobile technology develops increasing numbers of young people have access to the Internet through their phones, providing them with access to their email, social networking and gaming sites etc on the move.

No young person likes to be without his or her mobile phone at any time! Though every parent can be heard complaining about the bills, they can also be a good way of keeping in touch with family and friends, and ensuring that your child is safe.

What are the risks with mobile phones ?

Most new mobile phones are in fact mini computers in so much as they have web access, and more recently - mobile TV has been launched. This means that young people can access content from the Internet and TV wherever they are, and without parental or teacher supervision. With the advent of picture and video messaging - young people need to be increasingly careful about the images they share. It is very easy for inappropriate images to be shared around a number of phones, changed and even put online, where it is impossible to get back. This is particularly worrying, if images are used in child abuse sites. Young people also need to be aware that they put themselves at risk of mobile bullying, or inappropriate intimate contact if they give out their mobile number to people they don't fully trust.

There are now mobile phone operators who sell phones with filtering software included, so that young people won't access inappropriate websites or content. It is worth checking that your child's phone has this capability. Remind your child that any image they send on their mobile can be changed and shared online, and that once they have sent an image they have lost control of it. Read through the young people's website with your child, and help them to understand that they shouldn't give out personal details such as their mobile number to strangers, or other young people that they don't fully trust.

Cyberbullying

Children are using IT as part of their home and school lives from a very early age. Even if children do not have their own mobile phone parents will often let their children use their phones to entertain them (or keep them quiet!!) during car journeys etc. As such, most young people are very IT literate and familiar with the technology that has been described in this document. But as well as knowing how to use it, as they get older they also increasingly know how to exploit it to the detriment of other people. Whilst we have noted the risks of strangers gaining access to personal information and using this inappropriately, there is a significant increase in younger people abusing the information which they can access via the Internet and Mobile Telephones and using technology to facilitate the bullying of others.

This is called CYBERBULLYING which is explained as…….
"the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, which is intended to harm others"

There are different types of cyberbullying:
Threats and intimidation
Threats sent to people by mobile phone, email, or online.
Harassment or stalking
Repeated, prolonged, unwanted contact or monitoring of another person.
Vilification / defamation / prejudice-based bullying
These may be general insults or racist, homophobic or sexist bullying.
Ostracising / peer rejection / exclusion
Set up of a closed group refusing to acknowledge one user on purpose.
Identity theft, unauthorised access and impersonation
'Hacking' by finding out or guessing a username and password.
Publicly posting, sending or forwarding information or images
Disclosing information on a website.
Manipulation
May involve getting people to act or talk in a provocative way.

Unlike other forms of bullying (verbal, physical) there is no escape at home where they can be reached via the Internet and their Mobile. The bully can often remain anonymous but can reach a huge audience very quickly.

www.dizigen.org/cyberbullying/overview/how
provides lots of examples of how cyberbullying can take place, including misuse of webcams, gaming sites, consoles etc.

Civil and criminal law: Although bullying is not a specific criminal offence in UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications. In fact, some cyberbullying activities could be criminal offences under a range of different laws, including the Protection from Harassment Act 1997, which has both criminal and civil provision, the Malicious Communications Act 1988, section 127 of the Communications Act 2003, the Computer Misuse Act 1990 and the Public Order Act 1986.

What should I do……

- *If you start by telling your child never to do something most young people will ask "why not?" and then try to find out! Discussing the potential dangers with your young people therefore needs care and sensitivity and involves helping them to see for themselves how they might get into difficulty. Most young people will respond more positively if you encourage them rather than giving them a list of "Dos and don'ts"!.*
- *Teach them to respect others and always be careful what is said online and what images are posted.*
- *They must think before they send – once it is on the Internet or on a mobile telephone it can be made public instantly and could be manipulated.*
- *Advise them to treat their password like their toothbrush. Keep it to themselves. Don't make it easy to guess and change it as soon as they think it may have been compromised.*
- *Ensure they know how to block the bully.*
- *Don't retaliate or reply.*
- *Save the evidence and report it accordingly.*
- *Be aware that your child may as likely cyberbully as be a target of cyberbullying.. Be alert if your child is upset after using the Internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. They may be secretive about their online activities and mobile phone use.*

Contacts and Further Information:

Northumbria Police Community Support Officers www.northumbria.police.uk

Call 01289 307111

Child Exploitation and Online Protection www.ceop.gov.uk

Childnet International www.childnet.com

Becta www.becta.org.uk

Think U Know www.thinkuknow.co.uk

Digizen www.digizen.org

Parental controls will never make the internet 100% 'safe'. They should not be used as a substitute for communicating safety messages to your child. Make sure that you talk to your child about their behaviour online and remember, your home is not the only place they will be accessing the internet! (look at navigation bar).

Never ask your children to set these settings, if you are not confident in putting these in place ask a family friend or the shop assistant to help.

BT

BT‘s Security package is called **BT Family Protection**. This lets you choose the right level of protection for each child on up to three computers in your home. With this service you can:

Block websites – stop your kids from seeing inappropriate content
Set time limits – manage how long your children spend online
Get instant alerts – get email or text alerts when your kids try to view blocked sites or post confidential information
Social Networking tools – control the use of social networks like Facebook and Twitter and set up text alerts if personal information is posted
YouTube filtering – a unique technology to prevent exposure to unsuitable content
Usage reports – review your children's online activity from anywhere in the world

As well as parental controls, you also get:

Advanced spam filtering – with image blocking to protect children from offensive content
BT Cleanfeed – blocks sites classified as illegal by the Internet Watch Foundation
Access to our internet abuse prevention team – for children or parents to report any concerns
A user guide for the BT Family Protection service is available and videos on the service are also provided.

TALK TALK

Talk Talk’s Internet security service is called **HomeSafe**. Built into the broadband network itself, HomeSafe is designed to help you block every device in your home from websites you've defined as unsuitable for your home. Parents also have the option to control the after school homework routine specifically. It's been developed in partnership with their panel of parents and online safety experts. A guide to setting up HomeSafe is available as are videos for this service.

VIRGIN MEDIA

Parental Controls is part of Virgin Media Security and is available for free to all Virgin Media broadband customers. With **Virgin Media Security’s Parental Control** you can:

Screen out offensive material
Filter sites by pre-defined age categories
Add exceptions or block specific sites
Control access to specific content types like chat or social networking
Set an access-schedule for individual users
See a history of sites viewed, including those that were blocked
Further information on this service and a guide on how to set up parental controls is available.

PLUS NET

Plusnet offer **Plusnet Protect Internet security**. With this service, either offered free or for a small charge dependent on your Broadband package, parents and carers are able to set safe boundaries for children with parental controls.

SKY

Sky offer McAfee Internet Security available free or for a small monthly charge dependent on your Broadband package. Parental Controls are included in this package, however all Sky Broadband customers can get McAfee Parental Controls on their own as a separate download, free and for up to three PC's. McAfee's Parental Controls help control when your children can be online, monitor/control what websites they can visit, and keep an eye on their online activities.

DON'T FORGET THAT GAMES CONSULES ARE ALSO COMPUTERS THAT CONNECT TO THE INTERNET

For help and advice see the following websites:

X BOX

http://support.xbox.com/en-GB/billing-and-subscriptions/parental-controls/xbox-live-parental-control

PLAYSTATION 3

http://manuals.playstation.net/document/en/ps3/current/basicoperations/parentallock.html

Wii

http://www.nintendo.com/consumer/systems/wii/en_na/ht_settings.jsp?menu=pc

APPLE

http://www.apple.com/uk/search/?q=parental%20controls&section=global&geo=uk