Dear Parent/Guardian

1 in 4 young people have met up with someone that they first met online. How can you keep your child safe?

The Child Exploitation and Online Protection (CEOP) centre, is a Government run, multifaceted child protection agency for the UK. So far over 1 million young people nationwide have seen our thinkuknow education programme. This aims to empower and protect young people from the dangers of the internet through information and education. At CEOP we believe that every school should have e-safety at the top of their agenda.

Safer Internet Day (SID) is an annual event involving countries Europe-wide. SID 2011 is on 8th February and to highlight this, CEOP's Education Team have developed awareness raising assemblies. These are being delivered by schools across the UK during the month of February. Your son or daughter will be receiving this presentation in school and will be taught more about online and mobile communication technologies and how to stay safe whilst using them.

As a result of the assembly, your child may want to talk with you further about some of the issues raised. Young people are typically experts on the internet and parents may feel left behind, which can be disconcerting. We have developed resources specifically for parents to better equip you with the latest information to help you advise your child. By visiting **www.thinkuknow.co.uk**, you can enter the Purely for Parents area of our website which identifies and describes key communication technologies and how young people use them. You can also view our parents' guidance sheet which gives tips and suggestions of how best to look after your child's life online. Additionally you can register for monthly updates from CEOP, providing you with the latest information on internet safety and keeping your child safe.

Following the assembly, we recommend you discuss any outcomes with your child. You can visit the Thinkuknow website with them, allowing them to show you what they have learned.

We hope you take the time to use the resources and that your child enjoyed the presentation and has learned a lot from it.

Kind Regards,

Helen Penn

Head of Education

Child Exploitation and Online Protection Centre

Parent's Fact Sheet

Know what your children are doing online and who they are talking to. Ask them to teach you to use any applications you have never used. Keeping the computer in a family room means that you can share your child's online experience – and that they are less likely to act inappropriately (i.e. via webcam).

Help your children to understand that they should never give out personal details to online friends — personal information includes their messenger ID, email address, mobile number and any pictures of themselves, their family or friends. If your child publishes a picture or video online, anyone can change it or share it. Remind them that anyone may be looking at their images and one day a future employer could!

If your child receives spam/junk email & texts, remind them never to believe them, reply to them or use them. It's not a good idea for your child to open files that are from people they don't know. They won't know what they contain — it could be a virus, or worse — an inappropriate image or film. Help your child to understand that some people lie online and therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust.

Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable.

Teach young people how to block someone online and how to report them if they feel uncomfortable.

Websites:

www.ceop.gov.uk

www.thinkuknow.co.uk

www.getnetwise.org

www.theparentzone.co.uk

www.paceuk.info

www.internetmatters.org

Frequently Asked Questions

(Everything you wanted to know and were afraid to ask!)

Choose a topic below to reveal a list of common questions and answers that we have compiled. If you are looking for something specific and are not sure where to look then you could have a look at the full list here

Grooming Mobiles	Gaming	Social Networking	Chat
------------------	--------	-------------------	------

Grooming:

What is child sex abuse?

A child sex abuser (commonly referred to as a paedophile) is someone who is sexually attracted to a child or children and acts upon those desires.

Why do child sex abusers like to use the internet to contact children?

Child sex abusers find the internet an easier place to participate in a range of child sexual abuse activity including contact with children due to the anonymity of the medium. They will often lie and pretend to be younger than they are or people other than themselves, and find a sense of security by operating from the safety of their own homes. They have been known to set up bogus email accounts and chat personas to mask their identity online.

What are children at risk of, from child sex abusers, online?

There are a number of actions which these adults will engage in online. These include:

- Swapping child abuse images in chat areas or through instant messenger with other adults or young people and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught.
- Swapping personal information of children that they have collected with other abusers.
- Participating in online communities such as blogs, forums and chat rooms with the intention to groom children collect sexually explicit images and meet them to have sex.

What is online grooming?

The Sexual Offences Act 2003 defines online grooming as: "A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes."*

Often, adults who want to engage children in sexual acts, or talk to them for sexual gratification will seek out young people who desire friendship. They will often use a number of grooming techniques including building trust with the child through lying, creating different personas and then attempting to engage the child in more intimate forms of communication including compromising a child with the use of images and webcams. Child sex abusers will often use blackmail and guilt as methods of securing a meeting with the child.

*The full definition of Online Grooming can be found in the Sexual Offences Act 2003

Mobiles:

How do young people use 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 children have access to the internet through their phones, providing them with access to their email, social networking and gaming sites etc on the move.

Why is it good for young people to have a mobile phone?

No young person likes to be without their 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. The family of Milly Dowler, the teenager murdered on her way home from school has launched a campaign called 'teach ur mum 2 text' through the charity Milly's Fund in an attempt to help parents and their children keep in touch via text.

Sally and Bob Dowler's world was turned upside down when Milly went missing, but they knew they had to let her older sister, Gemma, go out and about like other 16 year-olds and wanted to find a safe and unobtrusive way to stay in touch with her. Text messaging was their solution. It meant they could keep each other posted but save Gemma the embarrassment of always being called by her parents. See www.millysfund.org.uk for more information.

What are the risks that young people encounter when using mobiles?

Apart from young people spending all their time chatting to their friends and not to you (!), there are some risks in their use of mobile technology. A large proportion of new mobile phones 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.

How can I reduce the risks to my children when they use their mobiles?

There are now mobile phone operators who sell phones with filtering software included, so that children 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.

Gaming:

Why do children and young people like to play games over the internet?

Gaming can be great fun, and can be a place where young people play and chat to each other. Gaming chat is often focused solely on the game, and young people will often swap user names to ensure that they can get to the next levels.

What are the risks to children and young people when gaming?

Gaming sites can be fantastic fun for young people, however as with any online technology - there are risks. The three main risks are:

- o Addiction
- Online gaming can occasionally be addictive for young people. They can become so involved in the gaming communities that they lose touch with their offline friends, in favour of spending time with online users playing games. Young people often spend hours every night playing games, especially when their parents have gone to bed. For this reason, CEOP recommends that the computer is kept in a family room. Parents will also then be able to monitor what games their children are playing, to ensure they are age appropriate.
- o Abuse
- Some young people who use online games can be abusive to other gamers. This can range from saying nasty things if there is a chat facility within the gaming site, to always winning and not sharing cheats or knowledge on how to progress to the next level. Young people should be encouraged that when they play online games, they treat others how they would like to be treated.
- o Risky behaviour
- There are some young people who engage in risky behaviour to obtain cheats or knowledge to progress within a game. Adults with a sexual interest in children will encourage them to engage in inappropriate behaviour for rewards including sexual acts via webcam or sex chat. Young people need to understand that their online behaviour has offline consequences and that if someone engages them in a sexual manner online that they should inform a trusted adult immediately.

How can I reduce the risks to my children when they are gaming online?

Playing games online can be a fantastic past-time for young people, but as parents you may not understand why your child spends so much time playing or how to help keep them safe.

It's a good idea to keep the computer in a family room. This is so you can monitor the games your child is playing online, to ensure they are age appropriate and also so your child won't engage in activities that could put them at risk. This also means that children will not have the opportunity to spend hours playing games in the privacy of their bedroom after you have gone to bed!

There are unfortunately some adults who have a sexual interest in children, and will use gaming as a means of grooming them. They may encourage young people to engage in inappropriate behaviour for rewards or cheats. Young people often don't understand enough about the risks and should be encouraged to talk to an adult they trust if they are engaged by someone in a gaming area. As a parent, it's vital that you talk to your child and make sure they know how they should behave when they are gaming. They should be encouraged not to accept cheats or talk to people that they don't know in the real world. If anyone asks them to do anything that makes them feel uncomfortable, they should tell a trusted adult or report their suspicions to CEOP on this website.

Social Networking:

What is social networking?

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.

What is a 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.

What is a 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.

What is an application?

An application is an enhancement that a user can choose to add to their profile to improve and increase interaction with other users in their contacts or networks. Young people enjoy using applications to share their interests with others. Examples include 'Top Friends', 'Where I've Been', 'Super Poke!', 'The Simpsons Quotes'.

What is a 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.

How do young people use blogs and social networking?

Firstly, they 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, and the school you go to. Most sites also have a blog (see 'What is a blog?' for definition) where children can write daily thoughts or include articles which they find interesting.

An important element in social networking is young people's ability to customise their 'space', e.g. by changing the colour of their profile, adding applications to their profiles, uploading images or pictures onto their profile. One of the pictures can be chosen to be the "default image" and this will be seen on the profile's main page. There is often also an option to upload videos as well – including music videos and personally recorded films.

What are the risks when social networking to children and young people?

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.

Do you have a case study to explain the risks posed to children when using social networking and IM?

Yes, the following is a composite case study, all names are fictional:

Olivia visited a chat room where she was talking to friends about her favourite band. A guy she hadn't met before read her profile and said hi. They started chatting, and Olivia got on really well with him - he seemed to agree with everything she thought and said which was cool. After some time, he asked her for her Instant Message address so they could chat more privately.

Olivia accepted him onto her contact list and after a few weeks of chatting through IM every day she felt she knew him pretty well. He sent a photo of himself to her and she thought he looked really nice, so when he asked her to send him a sexy photo of herself she felt apprehensive, but sent one anyway. He told her that she looked great and suggested meeting up.

Olivia felt quite uncomfortable with this, since she felt that he was still a stranger - however well they were getting on, so she refused but her new 'friend' got a upset with her and then aggressive and ended up saying that unless she agreed to meet up, he would send her sexy photo to all the people in the chat area.

Olivia was mortified, and really wasn't sure what to do; especially since she had started to worry about his intentions; not only was he blackmailing her but he was also making really suggestive comments which she felt very uneasy about.

One of Olivia's friends advised Olivia that she shouldn't have to put up with 'freaky guys' like this one, and told her to save her conversations with him, and report them to CEOP by pasting them onto the reporting form. This was then seen by a police officer who began to make enquiries and investigate further. Olivia was relieved that she didn't have to deal with the man on her own, and also found some great advice and support on the website.

Do you have any specific guidance for protecting children using social networking websites?

- Encourage them only to upload pictures that you as their parents / carer would be happy to see – 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 the school which your child attends since this could help someone locate them.
- Tell your children not to post their phone number or email address on their homepage.
- Help your child to adjust their account 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 your child has 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.
- Ask them to show you how to use a social networking site getting involved will empower them to share the experience with you.

Chat and Instant Messaging:

What is instant messaging?

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.

What is a buddy list?

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

What is a chat room?

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.

Are there different kinds of chat room?

Yes, 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. Its specific purpose is group communication in discussion forums or channels; however it also has the capacity for one-to-one communication via private message.

O 2D Visual Chat Rooms e.g. The Palace or The Manor – such 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 is an avatar?

An avatar is a graphical representation of a user. It can take the form of a 3D model of the user e.g. in computer games or a 2D icon e.g. on internet forums, chat rooms and instant messenger.

Why do children use chat rooms?

Chat rooms are usually areas where people meet to chat as they would in the real world in a youth club or bar. Young people love them because they are often unrestricted; and they can be exciting places to meet old and new friends.

Why do children use instant messenger?

Instant messenger is one of the most popular ways of chatting for young people. Often known as IM, this involves two or more people being online at the same time, and is different from chat rooms, because the people involved can only chat to people who are on their contact list. 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 the risks to children when using chat rooms or instant messenger?

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.

How can I minimise the risks to my children?

You can minimise the risks by taking the following simple measures with your children: 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 children 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 that your child 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 a child 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.

If you think your child may be in touch with an adult online make a report or call 999 if they are at immediate risk.

SMART thinking

		i
	Safe	WHO will see the information?
S	Keep safe by being careful not to give out personal information (such as name, email address, phone number, home address or school name) to people who you don't trust online.	WHAT will strangers do with the information?
	STOP and THINK	HOW can you stop strangers getting information about you?
	Meeting	WHY should you never arrange to meet anyone you don't know in the real world?
N	Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission, and even then only when they then go with you.	WHAT might happen if you do go and meet a stranger you have met on the internet?
	STOP and THINK	WHO should you tell and what should you do?
Α	Accepting	WHO sent it?
	Accepting emails, IM messages or opening files, pictures or texts from people you don't know or trust can lead to problems. They may contain viruses or nasty messages.	WILL it be safe to open?
	STOP and THINK	WHAT can I do to protect myself and my computer?
R	Reliable	WHETHER you can believe what strangers tell you when you are chatting to them online.
	Someone online may be lying about who they are, and information you find on the internet may not be reliable.	WHAT can I do to check they are who they say they are?
	STOP and THINK	WHAT can I do to check?
Т	Tell	WHAT can I when people I'm chatting to online make me feel
	Tell you parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. They can help you to report at www.thinkuknow.co.uk, and talk to	uncomfortable? WHO can I tell?
	someone who can help. STOP and THINK	WHAT can I do to stop it happening again?

Contacting Social Media Sites

If parents contact you about their children posting something they regret on Facebook, YouTube, Tumblr or another site you can refer them to this link for information on contacting social media sites:

http://www.thinkuknow.co.uk/14_plus/help/Contact-social-sites/

Contact social media sites

It's so easy to share online, that sometimes you might post something and wish you hadn't.

If you've posted something you regret on Facebook, YouTube, Tumblr or another site, you should delete it from your account as quickly as you can.

What if someone else has posted something about you?

Most websites have a way for you to ask them to remove 'content' – like videos, pictures, comments or profiles – that upsets you. This is called making a 'report'.

It's important to know that making a report doesn't mean the content will definitely be removed.

Just like in school, most websites have a set of rules - 'Terms of Use' - which they expect people using their site to obey. Websites will only take content down if they break these rules.

If you want to have something taken down from a site you should check to see if it breaks one of their rules.

Facebook calls their rules 'Community Standards', YouTube's rules are called 'Community Guidelines' and other sites like Tumblr, Twitter and Instagram have their own sets of rules and ways to report.

Before using any website you should read them to learn what is, and what isn't, acceptable on the site. You should also learn how to report content to the site.

Here's where to find the rules and how to report for the most popular social networks and messaging apps:

Facebook	Instagram
Read Facebook's rules	Read Instagram's rules
Report to Facebook	Report to Instagram
Facebook Safety Centre	Instagram Safety Centre
YouTube	Twitter
YouTube Read YouTube's rules	Twitter Read Twitter's rules

Tumblr

Read Tumblr's rules

Report to Tumblr by email

If you email <u>support@tumblr.com</u> about harassment:

Use the keyword "harassment" in your title and in your email.

Take a screen grab as evidence and attach it to your email

Put your Tumblr link and the details of the person harassing you in the email – give as much detail as possible.

Vine

Read Vine's rules

Contacting Vine and reporting

Kik Messenger

Read Kik's rules

Reporting to Kik

Kik Help Centre

Snapchat

Read Snapchat's rules

Reporting to Snapchat

Snapchat Help Centre

Ask.fm

Read Ask.fm's 'terms of service'

Read Ask.fm's safety tips

Reporting on Ask.fm:

You do not need to be logged into the site (i.e. a user) to report.

When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post for one of four reasons.

Spam or scam

Hate speech

Violence

Pornographic content

It is also possible to block other users, by scrolling to the bottom of their profile page and clicking on but users need to be logged in to do this. Users can also remove any questions from their own profile by clicking on the cross in the top right hand corner of every question and answer.

If you are using the app through Facebook, there is an option to report the application by clicking on "report/contact this app" which is displayed in the final tab in the right-hand column.

Otherwise, it appears that the block function acts a form of reporting, however, there is no evidence on the site that carrying out the blocking process alerts moderators to inappropriate content.

Dear Parent/Carer,

As you may have seen in the media, the Child Exploitation and Online Protection Centre (CEOP) has recently warned of a concerning increase in sexual offending on the internet involving webcams.

Today your child has attended an age appropriate assembly about how to stay safe when using webcams. We encourage you to support the messages they have received by emphasising:

- Always tell an adult you trust if you are being threatened online
- It is never too late to get help and support if this happens
- Offenders are committing a serious crime and will be pursued and prosecuted by the police
- Think before you go on webcam, never do anything which you wouldn't be happy for family or friends to see

Webcam abuse

CEOP have investigated a number of cases in which sex offenders have used extortion to force young people to perform sexual acts on webcam.

Typically online sexual extortion happens in the following way:

- An offender makes contact with a young person. This can happen anywhere online, including on a social network, in a chatroom, in a game or even on their mobile.
- The offender begins a conversation and tricks the young person into sending them an indecent picture, appearing naked or performing sexual acts on webcam. They trick them in a variety of ways including: pretending to be a girl or boy of the same age, pretending to be someone the child knows, flirting with them or sending them sexual pictures or videos.
- The offender records the webcam footage. They then threaten to share the video with the young person's friends or family if they don't perform more sexual acts. Some young people have been threatened for money or told to hurt themselves.

This has happened to hundreds, potentially thousands, of young people in this country.

This is sexual abuse. The emotional impact can be devastating. A number of young people have attempted suicide as a result of finding themselves in this situation.

To help prevent further harm, CEOP are calling on parents and carers to talk to their children about this type of crime and to support them to come forward should they find themselves in difficulty.

It's great to take an active interest in your child's life online and we'd encourage you to talk openly with them about the things they do. Remember, the internet is an essential part of young people's lives and provides them with tremendous opportunities. The vast majority use it without coming to any harm.

To start a conversation with your child you could tell them that you understand that some young people share sexual images and that you're interested to know what they think about it.

What to do if this happens

If your child were to tell you this has happened, your response as a parent will be crucial in helping them cope. It is important to take it very seriously whilst reacting calmly. When a child tells a parent they have experienced sexual abuse parents should:

- Believe their child and tell them that they believe them
- Not blame them for the abuse they have suffered.
- Tell them it's not their fault. Even if they have engaged in risky behaviour, the only person responsible is the offender.
- Not display anger or rejection even if they are feeling these things parents should work through them in a separate place
- Talk to their child about how they feel and let them know that they're here to listen.
- Report to CEOP. CEOP is a command of the National Crime Agency, and is dedicated to tackling the sexual abuse and exploitation of children and young people. CEOP is here to help young people (up to age 18) who have been forced or tricked into taking part in sexual activity with anyone online or in the real world. For information, advice and to report concerns directly to CEOP, visit www.ceop.police.uk



1. Watch your back

Whenever you're about to post something online, pause and just imagine someone in authority, someone you respect, reading that post or looking at that photo. If that feels uncomfortable, don't do it.

2. Got a nickname?

Think about using a nickname instead of your real name if you're signing up to a microblogging site like Twitter.

Consider setting up a separate, personal email account to use with social media sites, rather than using your work, or even your main personal email. Remember, only connect to people you know.

3. Check your settings

Use the privacy and security settings on social media sites so that only friends and family can see your pages.

Then speak to friends and family and encourage them to tighten their privacy settings too as they could affect you.

Even if your account is locked as private, personal information you have shared with others could still be accessed through their pages.

4. Mother's maiden name

Don't use your mother's real maiden name as a password or as a bank security answer. It doesn't really matter whether you use the real one so make up a name that only you know. Just make sure you remember it.

5. Guard personal information

Don't post any personal information- your address, email address or mobile number - publicly online. Just one piece of personal information could be used by a complete stranger to find out even more. If you want to include your birthday in your profile it's safer not to actually display it publicly - providing your full date of birth makes you more vulnerable to identity fraud.

6. Photos and videos

Be careful about which photos and videos you share on social media sites - avoid photos of your home, work, school or places you're associated with. Remember, once you've put a picture of yourself online, other people may be able to see it and download it - it may not just be yours anymore.

7. Check what's needed

Don't give out information online simply because it's asked for - think whether whoever is asking for it, really needs it. When you're filling in forms online, for example to register with a website or sign up for a newsletter, always provide the minimum information possible.

8. Direct message if you can

It's almost always possible to send a direct message or private message on social media platforms. If you're having a personal chat, this is the best option to go for - unless you don't mind sharing your conversation with millions of other users. Alternatively, send an email from a private account.

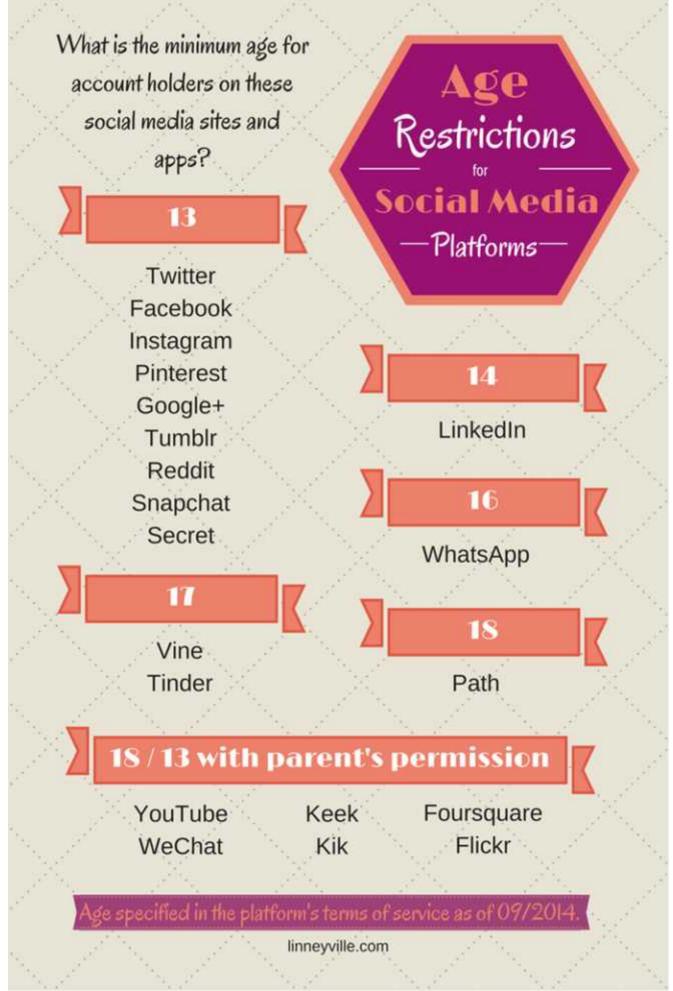
9. Delete old accounts

If you've stopped using a social media site or forum, then close your account down. There's no point in leaving personal information out there unnecessarily.

10. Get anti-virus software

Make sure you have anti-virus software installed on your computer and be careful what you download or install on your computer.

March 16



CHILDREN AND YOUNG PEOPLE ON WEBSITES

ADVICE FOR WEBSITE CREATORS

As a website editor you may be thinking of placing photos of children or young people on your website. However, there are important safety concerns to consider before doing so. Some of these may sound pretty obvious, nevertheless, it is vital that all those involved in designing and maintaining websites are vigilant and aware of the potential dangers associated with the posting of photos online. Schools and youth groups, for example, have a duty of care for their children - in other words it is their duty to ensure that every child in their care is safe. In the context of setting up a website this means that they must ensure that no individual child can be identified or contacted either via, or as a result of a visitor using the website.

BENEFITS OF SHARING PHOTOS

There are benefits as well as safety concerns in putting pictures of children on a website. For example:

- Web pages can be enhanced by photographs, and including photos can both enliven a page and make something appear more 'real'.
- Children and teenagers will be very excited to see a photo of themselves displayed on the Web. A picture of children, for example, together with references to their own achievements can boost the self-esteem of those photographed, allowing them to gain recognition for their achievements from their friends, family or other interested parties.

SAFETY CONCERNS

Placing photos on the web opens you or others portrayed in the photograph up to potential dangers such as from those wishing to exploit young people.

The key safety concerns here include:

- **Contact**: Children may be placed at risk by the provision of information on what they look like, which certain individuals may utilise to seek to identify and contact them in person.
- Bullying: Photos placed on the Internet have the potential to lead to bullying, which is harmful to children, lowering self-esteem and leading to higher levels of stress and anxiety. This may particularly be relevant to sites where visitors can post images
- **Distorting images**: Photos that have been put online may be altered and distorted. This could range from an image being altered in an unflattering way as a cruel joke (common with online bullies), morphed with another image to misrepresent or mislead or even used to create pornography (including child pornography).

CHILDNET'S VIEW

In developing your own website serious consideration needs to be given to the types of images you will include, the information accompanying these images and the legal issues surrounding the posting of photographs on the web. Attention needs to be paid to issues such as site security, permission to use the photos, the appropriateness of the photos and 'contactability' of the subject/s, and the moderating of images posted by visitors to the site.

Below is a checklist of issues to consider when thinking about putting photos of children on a website. It is important to consider these issues before putting the images online. Once an image is put online you lose control of it - it can be copied and sent to others very easily and very quickly.

CHECKLIST FOR PUTTING PHOTOS OF CHILDREN AND YOUNG PEOPLE ONLINE

- **Appropriateness of the photo**: If you decide to post photos online, it is important to be careful about how the individuals in it are portrayed. For example, pictures of children swimming or doing gymnastics are probably inappropriate.
- **Limit information accompanying the photo**: Posted photos should not be accompanied with any information which might allow the individual child to be identified. If a photo is posted, avoid identifying information including full name, or first name and class name etc. Similarly, if there are moving images then attention should be paid that identifying information is not include in the sound. Possibilities include providing just a first name or nickname, or a full name without the photo, and group photos are preferable to those of individual children.
- **The issue of contactability**: Individual contact details for children especially email addresses and phone numbers should never be given out on a website and in no circumstances be displayed under a photograph of the child.
- Permission to Use Photographs: Parental permission should be obtained before publishing any photographs of children on the website. The UK Department for Education and Skill's SuperHighway safety site gives some sample parental consent forms for using images of young children, see

http://safety.ngfl.gov.uk/schools/document.php3?D=d75.

The permission of the children should also be obtained.

- **Withdrawing photos**: As web editor, you should immediately remove all material relating to an individual on your website if requested by the legal guardian of the individual or by the individual themselves.
- **Moderation**: If people can upload content (including photos) to your site, then you need to ensure that users are aware of your guidelines and that you take a responsibility to filter/review this content and take down images where necessary.
- **Private access**: Consider using a photo-sharing package that offers password or other security protection. Some websites, for instance, create online photo albums that aren't visible to the public, and you can even choose the specific albums that you want to allow your friends and family to view.
- **Check the legal requirements**: Many countries have regulations in place for the protection of 'data' which are relevant here, for example the Data Protection Act 1998 in the UK.

For further information surrounding good practice and more guidelines for the creation of a safe website, there are some useful links listed below.

FURTHER INFORMATION

For further guidelines regarding the setting up of school websites see:

http://safety.ngfl.gov.uk/schools/document.php3?D=d72

• For more advice on the safety issues associated with the creation of websites see:

www.wiredsafety.org/safety/chat_safety/online_discussion_safety/

• For United States related information concerning the creation of web pages see:

www.deblogan.com/plan.html

• Some very clear and comprehensive guidelines for schools for the online publication of student images are provided by the New Zealand Ministry of Education, see:

www.tki.org.nz/r/governance/curriculum/copyguide e.php#four

• Further information regarding the Data Protection Act in the UK can be found at:

www.dataprotection.gov.uk

INFORMATION

CLICK CEOP Internet Safety www.ceop.police.uk/Ceop-Report	www.cybermentors.org.uk	www.iwf.org.uk Report online child sexual abuse images and videos
Chat room is open (between 8am - 2am) www.beatbullying.org	ChildLine 0800 mice The number won't appear on your phone bill	internet matters.org
www.thinkuknow.co.uk	www.youngminds.org.uk Telephone us: 020 7089 5050	NSPCC Cruelty to children must stop. FULL STOP. 0808 800 5000 www.nspcc.org.uk/internetSafety
KidSMART	Kine (IRall	UK Safer Internet Centre
www.kidsmart.org.uk	www.childnet.com/resources/kia/	www.saferinternet.org.uk