A parents' guide to E-Safety

Contents

Factsheets

PC Marcus Kudliskis

Safer Schools Police Officer

Harris Boys' and Girls' Academies, East Dulwich

m.kudliskis@harris-net.org.uk

Conversation starters

Let them teach you

The people who know best about what your children are up to online, are your children! Get them to tell you about the sites they're using. Ask them questions such as:

- Why do they like the site?
- What can they do on it?
- What's so fun about it?
- Who uses it at school?
- Who you can talk to?
- Who are their friends on it?

This is a good way to develop a trusting relationship with your child about what they are up to online.

Reach an agreement

A good way to set boundaries with your child about what they can and can't do online is to create an agreement with them.

Here are some examples of the areas you might want to discuss:

- Limits on the amount of time your child spends online, or playing computer games.
- Having regular screen breaks – at least five minutes every 45-60 minutes.
- Not sharing any pictures they wouldn't be happy to share with you.
- Not giving out personal details, such as mobile phone number and address, to people they don't know and trust.
- Coming to you if they are concerned. Or, if not, knowing where they can go for independent help and support.

Tips for helping your child to game safely

Just like with films, you should check the game's age rating before allowing your child to play. The Pan-European Gaming Information (PEGI) system sets age ratings for games and classify their content according to what is appropriate for different age groups. The rating will help you decide whether the game is suitable for your child. For information on game ratings visit the **PEGI** website.

Ask your child what is hot, and what is not! Get them to tell you about the game and, if they can bear it, play against them!

You might want to ask them:

- What they like about it?
- Which of their friends play it?
- Who are their friends in the game?
- To tell you about their character and profile.

It is important to stay up-to-date and regularly ask your children about the games they play and the people they are friends with.

When you know the kind of games your child is playing, go on and take a look.

Look to see if the game has advice for parents and carers. This can help you to assess the appropriateness and learn more about the functions of the site. In general, this advice tends to focus on the fun aspects of the game, but it should also highlight the safety measures the site has in place to protect your child and what you can do as a parent or carer to protect them, such as setting parental controls.

It is important that you read this information and learn how to report any issues directly to the site. This way you can help your child if they need it.

For more information about safe gaming, including setting parental controls on different games consoles, visit the **Association of UK Interactive Entertainment** site.

Most of the popular online games are played by adults and children alike. Therefore, your children need to be aware of the information that they share and the people they talk to.

It's never a good idea to share personal information such as their name, address, email address, passwords, telephone numbers or the name of their school with people they don't know and trust in the real world. Talk to your child about how people can sometimes lie online or pretend to be someone else.

Encourage your child to keep gaming friends 'in the game' and not to invite them to be friends on their social networks.

Some online games are virtual worlds which never end, where missions can take hours to complete. It's important to set limits on the amount of time your child spends playing online. Be aware of how long they spend gaming and set rules, as you would for TV. Also, ensure that they take regular screen breaks – at least five minutes every 45-60 minutes.

Talking to People

Young people use the internet to talk to others in a number of different ways: emailing, instant messaging, webcam and chat rooms. The online world provides young people with the opportunity to be inquisitive, explore relationships and actively seek risks, such as flirting with people that they don't know.

Chatting online feels different to chatting face-to-face. It can be easier to say and reveal things that you wouldn't in the real world, and be mean, aggressive or flirtatious.

It is important for young people to remember that there are offline consequences to online behaviours.

As a parent or carer, you need to understand the ways young people communicate with others, and the potential **risks**.

Until you feel your child is responsible and mature enough to understand and manage the **risks** of communicating with people they do not know, then you should restrict the sites they use and people they talk to. Young people should be aware that they can:

1. Block contacts. Most chat sites enable you to block contacts to prevent them from communicating with you.
2. Report contacts. If someone is being inappropriate on chat sites, you can often report this directly to the site administrator. However, if your child has experienced sexual or offensive chat that has made them feel uncomfortable or someone is trying to meet up with them, you can report this directly to **CEOP**.

Instant messaging (IM) is instant text chat between two or more people. This tends to be private un-moderated chat. You can build a list of 'friends' or 'buddies' that you can chat to, they can see when you are online and start conversations with you. It is important for young people to know how to manage this list, for example, blocking contacts they don't want to talk to.
Windows Live Messenger is a popular IM service; however, many sites, including Facebook, provide instant messaging.

SPIM is unsolicited messages that are sent through instant messaging sites. These could be adverts, scams, viruses or ways to gather your personal information for the purpose of fraud. Often these appear to be real people requesting to chat.
Your child should not click on messages and links from people that they do not know on their instant messaging accounts as they may risk their computer's security.

Webcams let you see the person you're talking to while you're chatting. Services like Skype are very popular and free. This can be a great way for young people to chat to each other; however, it is important to remember that what appears on webcam can be recorded and shared with other people in ways that you wouldn't want. Young people should be aware that it is never a good idea to reveal too much of themselves on webcam; this includes engaging in sexual behaviour.

A chat room is a forum where groups of people meet to chat online – this can sometimes be about a particular topic, or can be friends meeting to discuss something. Sometimes chat rooms are moderated; this means that someone, or a computer program, is looking out for inappropriate language or behaviour. Some chat rooms, even those aimed at young people, do contain a lot of sexual chat and online flirting. It is important for young people not to engage in sexual chat with people they do not know, or reveal too much about themselves.

These sites connect individuals at random with strangers to enable them to chat, either by text or webcam. The random element of connecting you with someone anywhere in the world is the main appeal of these sites

.

This type of site is often unmoderated and frequently used for chat and actions of a highly sexual and inappropriate nature which can be harmful to young people.

We would recommend restricting access to any site which randomly connects users to strangers

Socialising

Your child will be using services online to create a network of 'friends'. Social networking sites, like Facebook, encourage and enable your child to link with their friends so they can chat, keep up to date, share photos and videos... and their opinions of them!
Almost every site online now has a social element. Whether it is finding out what music your friends are buying, to reading their reviews of the latest films or games, increasingly we see the internet through the eyes of our friends.

To young people, their idea of an online 'friend' may be different to an offline 'friend'. Friends online might be your best mate, your entire school, friends of friends, people you meet gaming, or even just someone with a funny profile. Therefore, online 'friends' are likely to be a much larger group than friends in the real world.

Making someone your 'friend' gives them access to things you share – that could be; what you like, who you like and even where you live...Therefore, the larger the group of friends, the more people can see things about you. As you might expect, this can be risky, **for more information on risks, click here.**

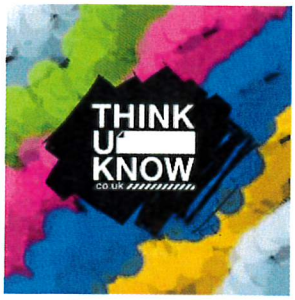
Here are four things you should discuss with your child to help them protect themselves when socialising online:

1. Know who your friends are. Because 'friends' have access to their personal information and can chat to them, your children should only be friends with people that they trust. Talk to your child about who their 'friends' are, encourage them to think about where and when they 'met' people and whether it is appropriate to share information with them.

2. Manage the information you share with them. On most sites, children can control the amount of information they share with different groups of friends. For example, you might share some holiday snaps just with your family, or create a private invitation to a party. Your child should only share personal information, like their telephone number or school, with people they know and trust in the real world. **More information on risks online**

3. Never meet up with someone you only know online. People might not always be who they say they are. Make sure your child understands that they should never meet up with anyone they only know online without taking a trusted adult with them.

4. Know what to do if someone upsets you. Sometimes 'friends' can do things that are upsetting, it's important that you and your child are aware of what you can do to block or report this – **click here more information on steps you can take**.



Searching for content

With a world of information at their fingertips, it's easy for young people to actively search for material that might be inappropriate for their age, or stumble across things that might upset or disturb them.

The internet can provide young people with unrestricted access to adult material. At an age where they are developing socially and sexually, it is natural for young people to be inquisitive. The internet can support natural exploration of sex, relationships and identity; however, there is the risk of exposure to material that could be detrimental to their development.

One of the ways to help manage what your child is exposed to online is the use of **parental controls**. These are a good tool available to you; however, they are not a substitute for talking to your child about what they see online.

It is likely that in adolescence your child will be curious about sex. They may well seek to explore this by looking at pornography. Pornography is big business online. It is quick to find, often free and has no age restrictions.

Pornography has always played a part in adolescent sexual development; however, the internet has significantly changed the type of content that young people are accessing. There is no top shelf on the internet and at the point at which young people are developing sexually, they can be exposed to material of an extreme nature – such as degrading, violent and dominating behaviours. This can result in: negative attitudes towards women, dysfunctional sexual attitudes and behaviours and unrealistic expectations of sexual relationships.

Difficult though it may be, you should talk to your child about pornography when you talk to them about sex. Emphasise that sex is part of healthy adult relationships, however, within pornography people are playing a role and the depictions of sex are unrealistic and potentially unhealthy.

If you are concerned about your child's use of pornography you can seek advice from your GP.

The Brook Advisory Service also provide help for under-25's with a range of sexual issues.

0808 802 1234

www.brook.org.uk

You can use the internet to find out about anything you are interested in and meet people interested in the same things, no matter how niche. Although this provides fantastic opportunities, it can also reinforce vulnerabilities. For example, some young people suffering from eating disorders have used the internet to promote these conditions to others as a lifestyle choice. Through these networks young people encourage each other to engage in unhealthy behaviours. This can reinforce their opinions about the illness and make it seem normal.

If you are concerned, visit B-eat **www.b-eat.co.uk**, who provide information for young people, parents and practitioners.

Anyone can create a website, it's easy and even the most extreme view can find an audience. At a time when young people's opinions are being formed, exposure to sites which convey extreme viewpoints may influence their views if not counterbalanced with other perspectives.

Encourage your child to talk to you about the things they read or see online. It's important to help your child understand that, just as national newspapers have their own political perspectives, websites may, and often will, have their own agendas. Just because it is online, it doesn't mean that it is true.

A lot of online content has been created by people like you and me. Websites like Wikipedia are written entirely by their users and this provides a great online resource. However, it is important for young people to know that not everything they read online is true. It may be a distorted opinion, or simply factually incorrect. 109% of people know this.

Encourage your child to check facts from other sources and also to think critically about sites they use.

.

Talk to your child about webcams

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.

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. We have also developed a fact sheet that you can share with your child with top tips on how they can *Stay Safe on Screen*, which you can download **here**.

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's Safety Centre**. If a child is in immediate danger please call the police on 999.
- Throughout September and October 2013, the NSPCC will also be running a dedicated 24/7 helpline on **0800 328 0904** offering help and support to victims of this type of crime and their famililes. Children can also get confidential help and support 24 hours a day by contacting ChildLine on **0800 11 11** or visiting **www.childline.org.uk**

Using a mobile phone

Most young people in secondary school own a mobile phone. The devices themselves are becoming ever more powerful and many offer the same functions you might have on a computer. Many mobile phones can now:

- **Access the internet** – this is no different to accessing the internet through a computer. Young people can go on any site that you can find online, including sites like Facebook, YouTube and also potentially age inappropriate sites.
- **Take and share photos and videos** – most phones have a fully functioning camera. Young people can take images and videos and these can be shared quickly, easily and for free through text message, email or uploading to the internet.
- **Chat with instant messaging, video and text** – young people can take part in private chats with people through their mobile phone.
- **Share your location** – through GPS, many phones can now identify their user's location in real time. This can then be shared on social networking sites and through other sites and applications.
- **Play games** – young people can use their mobile to play games and download new ones, sometimes these can come at a cost. See our **playing games section for more advice**
- **Add and buy 'apps'** – apps are programs that you can add to your phone that enable you to do a wide range of things, from playing simple games to finding up-to-date train times. Some of these apps have a cost.

With all of these functions available, talking to people is now only a small part of what mobile phones are used for. It can be difficult to keep tabs of what your child is up to on a mobile phone.

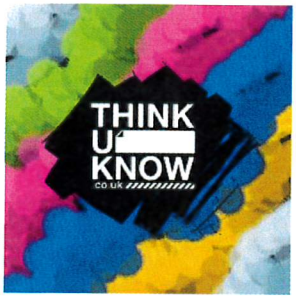
Parental settings – some mobile phone service providers allow you to set certain controls over your child's phone. This can include blocking access to certain sites and monitoring your child's activities. When buying a mobile, speak to the sales representative to find out more about what services they offer. You can find out more about what controls are available by looking at 'parents' sections online; here are a few to get you started:

- Vodafone - **http://parents.vodafone.com/mobile**
- O2 - **http://www.o2.co.uk/parents**
- T mobile - **http://www.t-mobile.co.uk/help-and-advice/advice-for-parents/**
- Orange - **http://www1.orange.co.uk/safety/**

Loopholes – even if you have set controls, your child may be accessing the internet through other sources. Many phones can access the internet through Wifi, which could be available on your street and picked up for free. Accessing someone else's Wifi may mean that your safety settings no longer apply.

Understand what your child's phone can do – all phones are different and you need to know what they are capable of so you can manage the risks.

Set a pin code on your child's phone – setting a pin code is like a password. Without a password, others may use your child's phone. This could enable them to access personal information, online accounts or run up expensive bills.



Set boundaries and monitor usage – this doesn't mean spying on your child! You can set rules with them about where it is used and how long for. For example, if you don't want your child to use their mobile at night, why not only charge it overnight in the living room?

Discuss what they can share – teach your child to think before they share online and the consequence of doing this over the mobile phone, such as **sharing their location**.

Discuss and monitor costs – phones can be expensive. As well as bills, costs can be run up through downloading apps, music or leaving data-roaming on abroad. Your child should be made aware of the financial responsibility that comes with owning a phone. There are different ways to manage costs, such having a contract or pay-as-you-go deals; make sure you discuss this in the shop.

Keep their mobile number private – young people need to understand that their phone number should only be given to people they know and trust, make sure that if they are concerned, they ask you first.

Be prepared in case the phone is lost or stolen – know who to contact to get the SIM card blocked. Every phone has a unique 'IMEI' number; make sure you write this down so if the phone is stolen, the police can identify the phone if they find it. You can get this by dialling *#06#.

Privacy settings and Parental controls

Most social networking sites, like Facebook, now give your child a lot of control over what they share and who they share it with. Through a site's 'privacy settings' you are able to control:

- **Who can search for you** – this means that when people search your name on a site, your profile does not come up.
- **Who sees what** – this means that you can control the information you share, like your photos or 'wall' posts. You can usually restrict this to friends only, friends of friends, certain groups of friends, or everyone. We would recommend that for young people it is restricted to friends only.
- **Who can post information about you** – some sites enable others to 'tag' photos of you or share other information about you, like your location. Many sites enable you to restrict people's ability to do this.

It is important that you stay up-to-date with the privacy settings that your child uses and help them stay in control of their profile. For more information about privacy settings in Facebook: **http://www.facebook.com/help/privacy**

As a parent or carer it can be difficult to monitor what your child is up to online. Most parents and carers trust their children online, but it can be easy for a child to stumble across things that might upset or disturb them.

Filtering and moderation packages are a good way to stop the majority of inappropriate and harmful content coming into your home. They are a tool to help you set and change online boundaries in line with your child's development.

There are some great packages out there, some are free and some come at a cost. Make sure you get one that suits your family's needs and budget.

Every parental control package is different, but most provide services such as:

- **Filtering** – content to restrict access to particular sites, such as pornographic websites.
- **Time limits** – restrict the amount of time your child can be online, or set periods of time where your child can access certain sites.
- **Monitoring** – where you are informed of certain sites that your child is attempting to gain access to.
- **Reporting** – where you are provided with information about what sites your child has used.

There are three main levels for applying parental controls.

- **Internet Service Providers (ISP's).** These are the organisations that pipe the internet to your home (like Virgin Media, Talk Talk, Sky and BT). All of the major ISP's provide parental control packages. These can allow you to apply controls across all of the devices that access the internet through your home connection – such as laptops or games consoles.
- **Devices that connect to the internet.** Most computers, mobiles and games consoles now come with parental controls that can be applied. For example, within Windows and the Mac operating systems, there are parental controls that can be set for individual devices.
- **Software.** There are a wide range of packages available to buy or sometimes download for free – always look for reputable companies and check out reviews online.

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.

Click here to view videos from BT, Virgin, Sky and Talk Talk on how to activate free parental controls from their services

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.

Plusnet

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 suit, 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.

Further information on **Sky's security packages** and a free download of the McAfee Parental Controls is available.

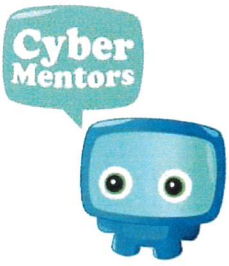
Contacts

Need someone to talk to?

You can talk to Childline about any problem you are worried about. They are available 24 hours a day and can talk to you in confidence. The number won't appear on your phone bill. You can call them for free on 0800 1111 or **visit their website**.

Are you being bullied?

If you are being bullied and need someone to talk to, you can find someone to talk to at **Cybermentors**, where there are people your own age and counsellors ready to listen and help.



Ceop……