

Safe Social Networking: Parental Workshop

Helping to keep your children safe online
Thursday 4th March @ 4pm



Aims of the session

- ✓ Reflect on the potential risks of internet use for children.
- ✓ Discuss the importance of communication with children about the time they are spending online.
- ✓ Understand how to set up parental controls on home and mobile devices.
- ✓ Know what to do if your child encounters problems online.
- ✓ Q&A





We understand that it is increasingly difficult to keep up with the ways our that our children are using new and ever changing technologies. Our children are **immersed** in a society that has become **dependent** on powerful computers, including smart phones, iPads, interactive online games and virtual communities.

This has become even more of an issue due to the global pandemic.



Children Online

Potential Risks

- ✓ Cyber bullying
- ✓ Grooming
- ✓ Inappropriate websites
- ✓ Losing control over pictures and video / Giving out too much information online
- ✓ Viruses, hacking and security



Risks of Gaming

- ✓ Many online games have communication features which allow their users to interact anonymously e.g. Minecraft (all devices) and World of Warcraft (PC) Roblox (app)
- ✓ Cyberbullies may harass fellow gamers and online scam artists may promise virtual goods in an effort to get credit card information e.g. World of Warcraft
- ✓ Some game consoles allow internet access as well, so it is important to be aware of their communication features.
- ✓ Expense - money - purchasing in apps
- ✓ Inappropriate content - GTA



Communication

- Be a part of their online life; involve the whole family and show an interest. Find out what sites they visit and what they love about them.
- No filter or parental controls tool is 100% effective, and many of the risks that young people face online are because of their own and other's behaviour.
- Create a family agreement for internet use, such as on <http://www.childnet.com/resources/know-it-all-for-parents/kiafp-cd>

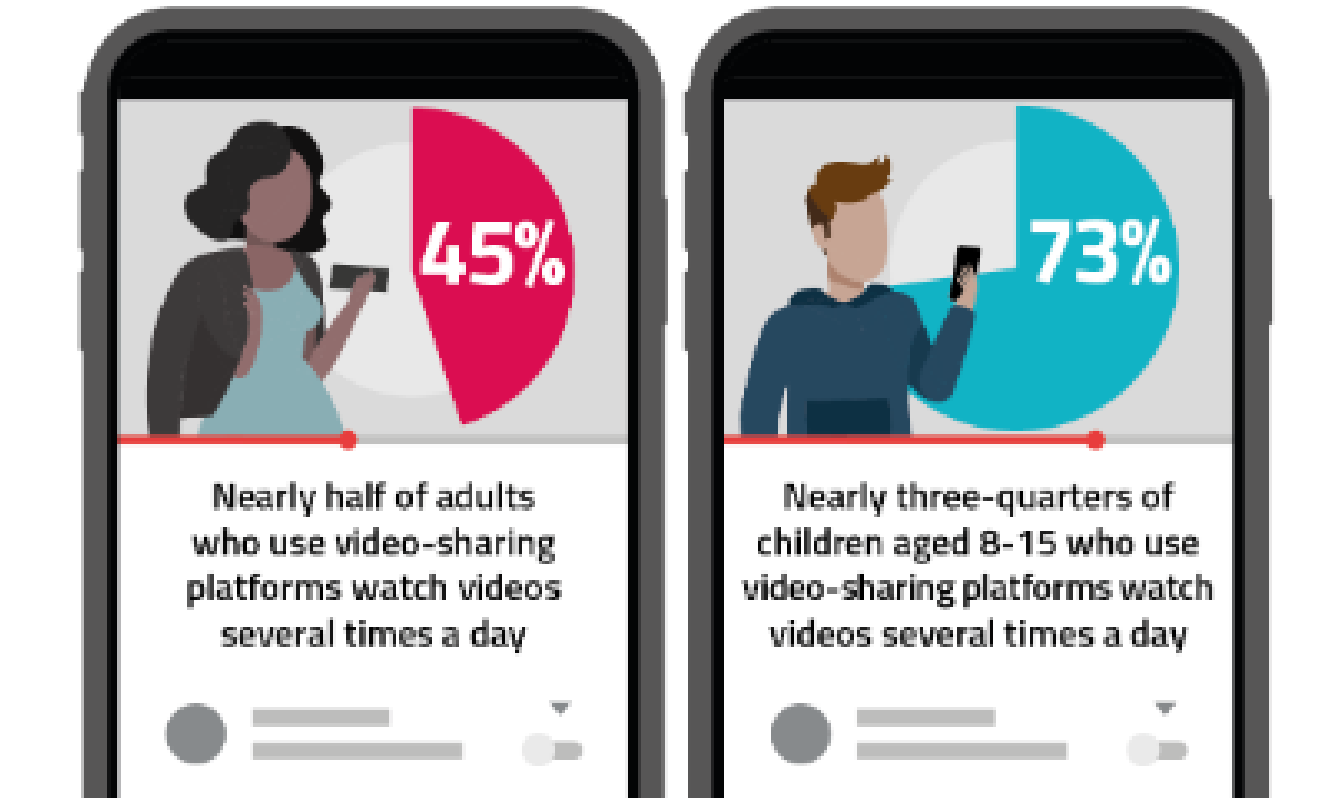


Websites such as Facebook, Instagram, Skype, Whats App, Viber and OoVoo, to name but a few, offer fantastic opportunities for communication and social connections. However, they are created with an audience in mind. This is especially relevant for sites such as **Facebook** and **Instagram**, which are specifically for those **over 13 years old**.

TIKTOK and Snapchat are a new concern.



Data from Ofcom



Users of Snapchat, TikTok, Instagram and YouTube who upload videos at least weekly

38% of adults



48% of children aged 8-15

28% of adults



50% of children aged 8-15

20% of adults



42% of children aged 8-15

9% of adults



16% of children aged 8-15

17% of adults who create and upload videos receive revenue or gifts in return



Issues we have faced since my arrival at the school:

Instagram - an online mobile photo sharing, video sharing and social networking service which enables its users to take pictures and videos and share them on a variety of social networking platforms.



You are required to be at least 13 years old before you can create an account.



TikTok

Tik Tok is a video streaming service. The legal age for using Tik Tok is 13 years old.

Common Sense (a media company) recommends the app for age 15+ mainly due to the privacy issues and mature content. **TikTok** requires that users be at least **13 years old** to use the full **TikTok** experience, although there is a way for younger kids to access the app.

- **Does TikTok have parental controls?**
- TikTok allows parents to set time limits, filter mature content, and disable direct messaging for kids' accounts. You can enable time limits and the content filter on your kid's phone and protect the settings with a passcode, but to disable direct messaging you need to use the app's Family Pairing feature. (Family Pairing also gives you access to time limits and content filter settings.) You'll need your kid's phone to sync the settings.
- Here's how to enable screen limits and filter content: Go to your kid's account and tap the three dots at the top right of the user profile. Then select "Digital Wellbeing" next to the icon of an umbrella. From there, select the features you want to enable:
- **Screen Time Management.** This setting limits users to a maximum of two hours on the app per day, but you can limit it to 40 minutes. If you're only enabling this on your kid's phone, choose a passcode to lock the setting.
- **Restricted Mode.** This blocks mature content, but even with the filter on, kids using the app on their own might come across age-inappropriate videos. Lock the setting with a passcode.



WhatsApp - An instant messaging app for smartphones. The user agreement requires users to be age 16 or older.



Other social media accounts to be wary of :



OoVoo which is a video and messaging app, it allows video chats of up to 12 people at one time. You are required to be at least 13 years old before you can create an account.



Skype - a video and messaging app. You are required to be at least 13 years old before you can create an account.



What are the implications?

Children are often creating 'groups' to which others are joining. This means that all information is shared with anyone who is in the group, so privacy is lost and in some cases strangers have been added to the group.



What are the implications?

- ✓ Many sites use 'targeted' advertising and therefore your child could be exposed to adverts of a sexual, or other inappropriate nature, depending on the age they stated when they registered.
- ✓ They may have lied about their age to get an account, making them appear older than they are, increasing this risk.
- ✓ Young people may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour. The general rule is, if they aren't friends in real life, they shouldn't be 'friends' online.



What are the implications?

- ✓ Language, games, groups and content posted or shared on social media is NOT moderated, and therefore can be offensive, illegal or unsuitable for young people.
- ✓ Photographs shared by users are NOT moderated and therefore young people could be exposed to inappropriate images or even post their own.
- ✓ Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and options.
- ✓ Social media sites can be exploited by bullies and for inappropriate contact. Social media sites cannot and do not verify its members, therefore, it is important to remember that if your son/daughter can lie about who they are online, so can anyone else.



What does this mean for you?

- ✓ Primarily, these occurrences and reported incidents of misuse of social media sites happen at home, after school hours when children have access to web sites that are blocked in school. With this in mind, and in response to concerned parents who have asked for advice regarding internet safety, we feel it important to point out to parents the risks of unregulated use of such sites, so you can make informed decisions as to whether to allow your child to have a profile or not and when and how to monitor their use, particularly at night time.
- ✓ We strongly advise a device free bedroom policy after bedtime to allow for uninterrupted sleep and rest.



Key point:

We cannot govern matters occurring out of school hours on the use of social media.

If we are made aware of them - we will educate the children and run sessions that week on the appropriate use of the internet and social media.

The use of netiquette. The etiquette used online.



Tips



- ✓ Keep the computer in a high-traffic area of your home.
- ✓ Establish limits for which online sites children may visit and for how long.
- ✓ Remember that Internet technology can be mobile, so make sure to monitor mobile phones, gaming devices, and laptops.
- ✓ Surf the Internet with your children and let them show you what they like to do online.
- ✓ Know who is connecting with your children online and set rules for social networking, instant messaging, e-mailing, online gaming, and using webcams.
- ✓ Check the browser search history on a regular basis.



Tips:

Should you decide to allow your child to have an online profile we strongly advise you:

- ✓ Check their profile is set to private and that only their friends can see information they post.
- ✓ Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting or messaging offensive/inappropriate messages or photos.
- ✓ Monitor your child's use of language and how they communicate to other people, ensuring profanity is discouraged.
- ✓ Have a look at advice for parents on the social media sites.
- ✓ Set up your own profiles so you understand how the site works and ask them to have you as their friend on their profile so you know what they are posting online.



Tips:

- ✓ Make sure your son/daughter understand the following rules:
- ✓ Always keep your profile private.
- ✓ Never accept friend you do not know in real life.
- ✓ Never post anything which could reveal your identity including photographs wearing school uniform where possible.
- ✓ Never post anything you wouldn't want your parents or teachers to see.
- ✓ Never agree to meet somebody you only know online without telling a trusted adult.
- ✓ Always tell someone if you feel threatened or someone upsets you.



Creating a Family Agreement

Staying Safe Online:

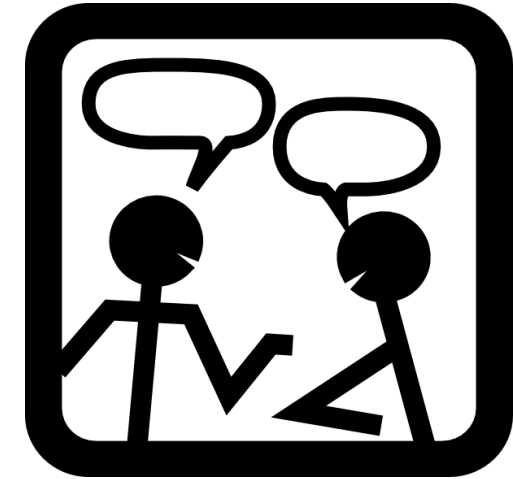
1. I will ALWAYS tell a parent or another adult immediately, if something is confusing or seems scary or threatening.
2. I will NEVER give out my full name, real address, telephone number, school name or location, schedule, password, or other identifying information when I'm online. I will check with an adult for any exceptions.
3. I will NEVER have a face-to-face meeting with someone I've met online.
4. I will NEVER respond online to any messages that use bad words or words that are scary, threatening, or just feel weird. If I get that kind of message, I'll print it out and tell an adult immediately. The adult can then contact the online service or appropriate agency. If I'm uncomfortable in a live chat room, I will use the "ignore" button.
5. I will NEVER go into a new online area that is going to cost additional money without first asking permission from my parent or teacher.
6. I will NEVER send a picture over the Internet or via regular mail to anyone without my parent's permission.
7. I will NOT give out a credit card number online without a parent present.

Young Person _____ Date _____

Parent/Guardian _____ Date _____



Discussion Starters



- ✓ What are your favourite things to do online?
- ✓ What is personal information? Why should you keep it private?
- ✓ What could you do to be safer online?
- ✓ What would you do if anyone online asked to meet you face-to-face?
- ✓ Besides me, who do you feel that you can talk to if you are in a scary or uncomfortable situation?
- ✓ Do you use IM or chat rooms to talk to your friends and others?
- ✓ How many people do you have on your buddy/contact list(s) and who are they?
- ✓ Have you ever chatted with someone you did not know in real life? What kinds of things did you talk about?
- ✓ Do you know how to block others in chat rooms and IM? Can you show me how to do this?
- ✓ Go to <http://www.netsmartz.org/InternetSafety> for further examples.



Parental Controls

Internet Providers

- ✓ The 5 big internet providers in the UK - **BT, Sky, TalkTalk, Plusnet** and **Virgin Media** - provide their customers with free parental controls.
- ✓ These providers offer filter levels e.g. BT provides 'light', 'moderate' or 'strict' filter levels.
- ✓ Parents can :
 - ✓ customise their parental controls.
 - ✓ allow and block specific sites.
 - ✓ set filter times.
 - ✓ set limits for time online.



Parental Controls

Gaming Devices

- ✓ Parental controls can also be set up on games consoles, such as Playstation, Xbox and Nintendo Wii.
- ✓ Restrict games based on age rating.
- ✓ Restrict time spent e.g. On the Xbox 360 activate the "Family Timer" to limit the total amount.
- ✓ Control your child's friend requests so you know who they're playing with online.
- ✓ Restrict online user-to-user communication and the exchange of user-generated content.



Parental Controls

Smartphones



- ✓ Capable of a range of internet functions: social networking, listening to music, playing games, browsing the internet, checking emails, taking photos and videos and watching TV.
- ✓ Out and about, users access the internet via 4G/5G connection which is provided by the data allowance in their mobile contract.
- ✓ All mobile network providers provide parental controls.
- ✓ Some will have these on as default, but others you will need to request to be turned on.

e.g. Tesco Mobile and O2 have a parental control option to ensure that only websites they have classified as suitable for children under 12 can be accessed.

Contact your service provider to find out about filtering options.



Parental Controls

Smartphones

- ✓ Internet on smartphones can be accessed by Wi-Fi from home, therefore home internet controls apply.
- ✓ Some apps can help filter out age-inappropriate content or help restrict some of the smartphone functions, so have a look in the app store.
- ✓ Check what parental controls are available for the specific smartphone; some devices may have options for switching off the internet browser.



Parental Controls

iPads

- ✓ Look at age ratings and customer reviews before your child downloads an app.
- ✓ There are tools available which can block some communication apps. For example there are parental control settings on the iPad to disable the following functions:
 - ✓ FaceTime: a video calling app
 - ✓ Ping: an instant messaging app
- ✓ Multiplayer gaming: You can choose settings to prevent multiplayer games and adding friends. Find the parental control settings and in the Game Centre section select 'Off' for 'Multiplayer Games' and 'Adding Friends'.



What to do if your child sees inappropriate material online?

- ✓ Don't overreact if your child tells you about something they have seen. You might feel shocked and angry but by dealing with it calmly your child will know they can turn to you again.
- ✓ Keep records of abusive messaging.
- ✓ Report abusive or inappropriate behaviour to the website and if serious, to the police.
- ✓ If you come across illegal content, such as images of child abuse, you can report this to the Internet Watch Foundation at www.iwf.org.uk.



Our support

We recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online www.thinkuknow.co.uk, www.net-aware.org.uk and www.getsafeonline.org



Get Safe Online
Free expert advice

Useful Websites

- www.saferinternet.org.uk/advice-and-resources/a-parents-guide/internet-enabled-devices
- www.kidsmart.org.uk/beingsmart
- www.childnet.com/resources/parental-controls
- <https://www.thinkuknow.co.uk/parents/Primary/>
- <http://www.netsmartz.org/Parents>



Final thought

We are here to promote the safe and responsible use of the internet. However, it is only through a collaborative effort between parents and teachers that we will succeed in creating responsible and safe cyber citizens.

