ONLINE SAFETY FACTSHEET

Introduction

For children and young people the internet, and the increasing number of digital devices they use to connect to it, is a part of their everyday lives. Whether they use it to express themselves or to stay in touch with friends, for entertainment or education, the internet can provide tremendous benefits and most use it safely. But while digital technology provides a wealth of opportunities, we are all aware that there are online risks and sometimes these risks can lead to harm.

At the same time, while young people's 'offline' and 'online' worlds are often merging, the behaviour and safeguards of the 'real' world are not always applied in a 'virtual' world where friends can be added at the click of button and information shared in an instant.

This guide aims to help parents consider some of the risks of the virtual world and how they can help their children be safe online.

Online Chatting

There are lots of different ways children and young people can chat online - and lots of different places it can be done. Chatting includes any type of service which allows your child to have a conversation with somebody else. It can be text based messaging (such as instant messaging, BBM or SMS) or via a voice or video link (such as by Face Time, Snap Chat, Instagram). It can also be instant, real-time communication (chat rooms or instant messaging) or delayed (such as e-mail or voicemail). Chatting like this is a great way to stay in touch - as well as meet new people. But there are a few things you can do to make sure your child is safe:-

- Know who they are talking to online; if they don't already know someone face to face they could be anyone; encourage them to think before talking to people they don't know in person
- Remind them that what they do or show on a webcam or video link can be recorded and what they see from the other end might be a recording
- Encourage them to avoid having one-sided webcam conversations where the other person's webcam is 'broken' or, 'not working…'; you won't know who they really are, what they are doing or who they are watching with
- Remind your child to keep their personal information private - avoid sharing personal information such as phone number, home address or photographs with people you don't know in person and trust
- Check whether the service they use allows them to create friend lists; these lists let them manage who sees what

- Private messages should be used for people they know in person and trust; tell them to be careful of private messaging people they don't know
- Encourage them to use a strong and unique password for all of their online accounts – a combination of letters, numbers and symbols (and if they've ever shared it in the past, change it now)
- Make sure they know how to block someone if they make you feel uncomfortable or upset; if they don't, help them to learn how to use the blocking feature
- Teach them how to save chat logs and texts so that if someone does make them uncomfortable/upset, they have the evidence to report them
- Remind them to log out of a service properly after use, especially on a shared computer
- Try to understand and guide your child's online behaviour - negotiate and establish boundaries and discuss sensitively the issues around the concept of 'friends'
- Familiarise yourself with the chat programme your child uses. Find out more about its built-in safety functions and how they can be contacted within the service
- Ask your child if they know how to block someone who they don't want to talk to anymore. ☐ Use parental control software provided by your internet service provider, mobile phone network, online content provider or games console and consider using filtering options, monitoring and setting time limits for access to chat
- If you discover misconduct between your child and someone online stay calm, investigate the facts and seek expert help where needed
- As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality, which may include sexual chatting and encouraging others to engage in sexual activity

Online Sharing

If children have something they feel proud or a view they want to express of then it can feel good to share it with others; maybe it's a photo they've taken or a video they've made. One of the great things about sharing on the internet is that it's quick and easy - you just click a button on your computer, smartphone or digital camera and it's there online. But that can also be a problem. If they post something in haste they may regret it later and by that time it may be too late to get it back. Here are some things you should encourage your child to think about before they ever share anything online:-

- Once it's shared online you've lost control and ownership of it; the image can be downloaded and used by others once it is on the web and has no protection – make sure you and your children know how to use the privacy settings on the service you use and set then; these

settings will help you take control of your information so that you can decide what information you will share, and who you will share it with

- Remember people may still be able to see the things shared online months or even years into the future
- A good question to get children to consider before putting an image or view online is - 'Would I share this with my parents/carers/teacher?' - if they wouldn't, then they shouldn't share it online
- Some people could use information or things you've shared in ways you don't like or couldn't have imagined
- Set up a family email address you can all use to fill in online forms
- Set clear guidelines for your children about what is ok to share about themselves and about your family – lead by example and explain what you have shared and why; be aware that comments posted by your children could impact on you and your family's reputation
- Talk to your children about how easy it is for people to assume another identity online
- There are a number of ways that you can set your own lists of sites you want to block access to; activating your internet service provider's parental controls, or those of another provider, can make this easy for you
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date
- Be aware that children can access the internet through publicly available Wi-Fi for example in shops, coffee bars etc; check whether your children's devices have built in Wi-Fi connectivity and see if there are any tools to help manage access to inappropriate content
- As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality which may include sharing sexual images
- Be aware that smartphones often contain location technology. This technology finds the mobile's position and provides services related to where you are. Talk to your child about who they share this information with

Online Gaming

Playing games online against other people can be really enjoyable and great fun. You can do it via a mobile phone, a computer or a games console and online games come in every shape and form. Online gaming has something for everyone and millions of children and young people across the UK regularly take part. Below are some tips to ensure children get the most out of their online gaming experience.

- Encourage them to keep gaming friends 'in the game' – avoid sharing personal information with people and avoid giving out social networking

profile details or email address; choose a user name that does not reveal any personal information about you

- Use a strong and unique password for all of online accounts – a combination of letters, numbers and symbols (and if they've ever shared your password in the past, change it)
- Teach them how to block people they don't want to be in contact with any more. If they experience any bullying, hacking or racism, make sure they know to save the evidence and report it
- Remind them to always log out of a service properly after use, especially on a shared computer
- Use the PEGI games ratings to guide you when buying games for your child or making judgements about the games they are playing. The PEGI system rates video games at various age levels (3, 7, 12, 16 and 18) and is designed to protect children and young teenagers from inappropriate content
- Make sure your children are using games from reputable and legal online providers
- Online gaming can be compulsive for some; be aware of the amount of time spent online and set boundaries around your child's use - games should be played as part of a healthy and balanced lifestyle; regular 5 minute breaks should therefore be taken every 45 minutes to an hour
- Use parental controls on games consoles to disable or restrict access to facilities such as voice chat. They can also be used to disable online credit payments or applications that you feel are inappropriate
- You can use online parental controls to restrict or block access to online gaming websites and other content altogether
- Familiarise yourself with the chat programme your child uses. Find out more about its built-in safety functions and how they can be contacted within the service
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date

Online Networking

Online communities - such as social networking sites - are some of the most popular sites on the web. Millions of people log onto these sites every day to hang out with their friends and talk about their lives. When you sign up you get the chance to create and customise your own profile and you can upload your favourite photos and videos. There are even networks within networks where you can join others who share the same interests, or who live in the same area or go to your school. Most people will have a great time being a member of these sites - but it's important you take care, particularly when giving out information about yourself. Here are some tips on how children can network safely:-

- Remind children and young people that adding someone as a 'friend' means they (and sometimes their friends) may be able to see the things you share, share things with you and even share things about you; can you trust them with your information?
- It's easy to lie online, not everyone is who they say they are – your children need to know this
- Teach children about privacy settings to take control of their information and help them to decide what information they will share, and who they will share it with
- Advise them to avoid friending people they don't know in person and not to share personal information with them such as their phone number, home address or photographs
- Keep an open dialogue with your child about who they're talking to online and why they should think before talking to people they don't know in person; try to understand and guide their online behaviour just as you would for their offline activity; negotiate and establish boundaries and discuss sensitively the issues around the concept of 'friends' (and 'friends of friends')
- Use parental controls to restrict or block access to social networking sites; device-level parental controls mean you can set up unique settings per user so that you can restrict access to particular networks based on the user
- Explain why it's important to be honest about your age online, for example in signing up to social networking sites – advertising and other content will be aimed at the age the user says they are
- Talk about what they should do if someone asks to meet them face to face

Additional Web Resources

- CEOP for Parents and Carers
- BBC WebWise – online safety advice for parents
- Keeping your child safe online
- www.o2.co.uk/parents