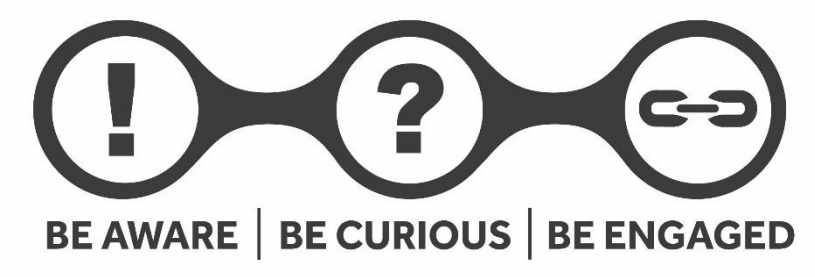
Quick guide for Parents and Carers

How to support children to stay safe online

Be a part of your child's online life; involve the whole family and show an interest. Find out about the sites they visit and what they love about them, if they know you understand they are more likely to come to you if they have any problems.



The 3Ws, questions to explore with your child

Where (is my child going online)	**Who** (*are they talking to online*)	**What** (*are they doing online*)
I know you love going online, which bits do you like best?	Do you really know everybody on your friends list?	Do you know how to use the privacy settings?
Do you think you can be recognised through your photos?	Do you ever get messages from strangers? What do you do with them?	What made you choose that photo for your profile image?
What do your friends like doing online?	Has anyone online asked you for a photograph or webcam image of yourself?	Are those your comments? Does James always post comments like that?
Have you ever googled your name?		Have you uploaded any videos of you and your friends online?

"Be curious, not judgmental."

Walt Whitman

What makes some online spaces more of a risk than others?

Anonymous Chat	
	**YikYak –** location aware for contact within a 5 mile radius
	**Ask.fm** – post selfies and talk about themselves
	**Omegele** – linking strangers together anonymously in chat or video rooms
	**Whisper** - A social "confessional" app users type a confession, add a background image and share it with the Whisper community. Intended for users age 17 and older.
Temporary Apps	
	**Snapchat -** messaging app that lets users put a time limit on the pictures and videos they send before they disappear.
	**KIK -** app-based alternative for texting and social networking. Users ask “Whats your KIK” to request usernames which can be found through other apps i.e. Instagram
	**Burn Note** - texting-only app that erases messages after a set period of time. Messages are stored until first view and then deleted.
Live Streaming	
	Periscope – users broadcast themselves live for short periods of time
	Meerkat – additional tools allow saving of live stream and live chat

	Facetime – iOS app built in to Apple devices
	Facebook Messenger - available to all Facebook account holders
Photo Sharing	
	Instagram - users often list their Kik usernames in their bios so that others have some kind of way to contact them privately
	Tumblr – popular blogging platform largely dominated by visual content
	WhatsApp - extremely popular app for individual and group messaging. Groups of up to 256 people can be contacted at the same time
Peer to Peer	
	BearShare – beware! Known for installing malware and other nasties on computers
	eMule – used to find 'rare content'. Fake versions ask for credit card details and distribute malware
	KCeasy – free to download software making it easier to access and share files

Phishing *(n): trying to get access to personal information usernames, passwords, bank details etc.) using fake emails, websites or posts*

Getting taken in by phishing can be serious, so it's good to know how to detect it.
These tips can help you to spot online scams.

- **Check the URL -** The URL on a phishing site may have missing letters or be spelled incorrectly
- **Watch out for pop-ups**. they can be used for phishing or to download harmful software onto your device
- **Be wary of 'free' stuff –** Don't trust offers that sound too good to be true, like winning free gadgets or making loads of money
- **Don't fall for requests to confirm your details** - Legitimate online services won't ask for your password or bank details by email

The Dark Web

The dark web refers to websites which are hidden by encryption through something called an 'onion network' because internet traffic is disguised by going through lots of layers, like the layers of an onion. TOR The Onion Router is the most well-known encrypted browser. It's not illegal to download it. An encrypted browser keeps internet activity anonymous, so it's very popular with people concerned about online privacy.
In 2014 the University of Portsmouth found child pornography the most requested type of content. Drug dealers can trade easily and political and religious extremists communicate freely using the dark web. Jamie Bartlett

author of The Dark Net would argue that parents should explore the dark web and discuss with older children what they might find if they go there.

Advice for Parents

NSPCC Net Aware – searchable guide for apps popular with children
http://www.net-aware.org.uk/#

Internet Matters – chatting apps popular with children and young people. Privacy setting guides for the apps if available
http://www.internetmatters.org/advice/apps-guide/

Parent Zone – guide for parents of under 13s using social media apps
http://parentzone.org.uk/article/under-13s-and-social-media

Keeping Under Fives Safe Online –
http://www.childnet.com/ufiles/Keeping-Under-Fives-Safe-Online.pdf

What is Sexting?

- Exchanging images of a sexual nature with a boyfriend or girlfriend.
- Sharing images of a sexual nature with someone you like.
- Passing on images of a sexual nature to groups of friends without permission.
- Sexting could be a nude or provocative picture in their underwear or a rude text or video.

Should parents be concerned?

You - or your child - could be breaking the law by taking, holding or sharing indecent images of a minor. Any image of a person under-18 sent may constitute an indecent image of a child, in legal terms, and be prosecutable under the Protection of Children Act 1978. Sexting can be an aspect of bullying.

Sexting and Revenge Porn

You may have seen an advertising campaign highlighting the new criminal offence of 'revenge porn'. The new law covers images shared by adults (over 18s) on social media and websites, via email or offline. Sometimes this material is sent to family members. The aim is to embarrass, shame and cause distress. The law is designed to counter the idea that the images are the fault of victims and to encourage them to come forward.

Some revenge porn sites boast that they feature teen revenge porn, despite the fact that sharing sexual images of under-18s has long been illegal. The sites attempt to blur the distinctions between over-18s and under-18s, reflecting the fact that there is a market for images that are intended to shame young people.

Advice for Parents

NSPCC - http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/

NSPCC – PANTS questions answered http://tinyurl.com/z4tn23c

NSPCC – How to talk PANTS http://tinyurl.com/jrgcpg8

The Zipit App from Childline -
http://www.childline.org.uk/Play/GetInvolved/Pages/sexting-zipit-app.aspx
ThinkUKnow - https://www.thinkuknow.co.uk/parents/article-repository/Nude-selfies-a-parents-guide/
Revenge Porn Helpline - http://www.revengepornhelpline.org.uk

Online Bullying – Practical Steps

- Find out what exactly has been happening. Keep a record of all incidents and when they occurred
- Take screenshots of any messages before deleting them
- Block and report anyone who's been bullying your child online
- Change any passwords that might have been compromised by online bullying and check privacy settings
- Don't confiscate your child's device or stop them spending time online
- Make a plan for where your child can go to escape bullying at school
- Make sure your child's school is aware – even if it's been happening outside school

Advice for Parents

ParentInfo - http://parentinfo.org/article/understanding-online-shaming-a-guide-for-parents

The Diana Award's anti-bullying campaign -
www.antibullyingpro.com

The Anti Bullying Alliance - www.anti-bullyingalliance.org.uk

NSPCC - https://nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/research-and-resources/

Selfie **(n): a picture of person taken by that person**

Recent figures show that 91% of teens have taken a selfie and over 1 million are taken each day

Young people sometimes forget that this isn't real and compare themselves, (complete with flaws and bad days) to others perfected online versions of themselves, they can start to feel inferior and not as good as everyone else.

Remind young people that comparing themselves to others on social media is not helpful, they're comparing themselves to something impossible and unattainable - nobody looks fantastic all the time and everyone has bad days.

The Gaming Environment

Some video games teach children the wrong values:

- Violent behaviour, vengeance and aggression are rewarded
- Women are often portrayed as weaker characters or as sexually provocative
- When playing online, your child can pick up bad language and behaviour from others

Video games can also:

- Confuse reality and fantasy
- Make your child vulnerable to online dangers
- Cause impulsive behaviour (linked to excessive use)
- Increase attention, physical and mental health problems

PEGI Ratings

Bad Language
Game contains bad language

Discrimination
Game contains depictions of, or material which may encourage, discrimination

Drugs
Game refers to or depicts the Use of drugs

Fear
Game may be frightening or scary for young children

Gambling
Games that encourage or teach gambling

Sex
Game depicts nudity and/or sexual behaviour or references

Violence
Game contains depictions of violence

Online gameplay
Game can be played online

The PEGI labels appear on packaging indicating an age level. They provide a reliable indication of the suitability of the game content in terms of protection of minors. The age rating does not take into account the difficulty level or skills required to play a game. There is also a PEGI app to help you understand the rating symbols.

Advice for Parents

Ask about games - http://www.askaboutgames.com

PEGI Ratings - http://www.pegi.info/en/index/id/23

Common Sense Media -
https://www.commonsensemedia.org/blog/gaming-tips

CEOP

The ‘report abuse’ button, allows children and young people to report suspicious individuals or behaviour directly to law enforcement quickly and easily.

The reports go directly to the CEOP intelligence centre and the team can analyse, assess and take appropriate action according to the perceived risk and threat to an individual child.

Reports are always investigated and it is very important that the service is not misused.

Managing Access

Parental controls are tools to help you manage your child’s internet use. There are lots of different types – you can set them at network level, on your child’s device or in an individual app or service. They help make sure your child has access to age appropriate apps and games and make it safer for them to browse the internet.

Parental controls can:

- Block and filter inappropriate content
- Restrict what information your child can share
- Control when and for how long your children can go online
- Be customised for each family member

Advice for Parents

Setting up Parental Controls through your Internet Provider

http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/parental-controls

Guidance for many games consoles and devices -
http://www.internetmatters.org/parental-controls/devices-computers/

Amazon Prime, one of the more difficult to find! -
https://www.amazon.co.uk/gp/help/customer/display.html/ref=hp_ab_link_n_201423060?ie=UTF8&nodeId=201423060&qid=1454429529&sr=13-2-acs

FOMO – Fear of Missing Out

FOMO is used to describe the feeling of anxiety that an exciting or interesting event may currently be happening elsewhere, often provoked by posts seen on social media.

These tips may be useful for helping your child if they are affected by FOMO:

Listen. It can be easy to dismiss FOMO and other social media stress as superficial, but for many tweens and teens, social media *is* social life. The more you show you care about how they feel, the more open they'll be.

Don't judge. For tweens and teens, connecting with their peers is a normal part of child development. For current parents, it may have meant hours on the phone.

Encourage their offline lives. FOMO can chip away at kids' self-esteem, but the best defence is a strong sense of what makes kids unique, worthy, and valuable. Help them participate in sports or drama clubs.

Set limits. After all the listening and validating is over, set some basic limits around when and where the phone or computer can be used. Start with turning phones off an hour before bedtime. You can suggest they tell their friends they'll be signing off at a specific time, so they won't be expecting a response

Ideas for Family Rules

Your child's use of technology is on an ‘agreement based on trust’ arrangement

Check with your child regularly about who and what they are doing

Have them teach you about their favourite online websites, apps and forums

Be their online ‘friend’

Discuss and use parental controls

Talk openly about the potential misuse and responsible use of the resources online

Advice for Parents - Parental Controls and Family Agreements

http://ourpact.com/

http://www.breckfoundation.org/technology-safety-contract.html

http://www.digizen.org/digicentral/family-agreement.aspx

https://www.commonsensemedia.org/sites/default/files/uploads/connecting_families/family_media_agreements_k-12.pdf