



Online-Safety

A briefing for Parents













School

Almost 1 in 4 of 8 to 11-year-olds and 3 in 4 of 12 to 15-yearolds has a social media profile



1 in 3 internet users are children



Source: Ofcom (2017) Children and parents: media use and attitudes report (PDF).



Source: Livingstone, S., Carr, J. and Byrne, J. (2015) One in three: internet governance and children's rights (PDF).
Ontario: Centre for International Governance Innovation.



1 in 4 children have experienced something upsetting on a social networking site.



Source: Lilley, C., Ball, R. and Vernon, H. (2014) The experiences of 11-16 year olds on social networking sites.















School

There were over

2,100

counselling sessions with

young people who talked in

Childline about

online child

sexual

exploitation

(CSE) in 2016/17



In 2016, the Internet Watch Foundation

identified **OVE**

57,000 URLs

containing child sexual abuse images



Source: Internet Watch Foundation (IWF) (2017) Annual report 2016 (PDF).



Source: Bentley, H. et al (2017) How safe are our children? The most comprehensive overview of child protection in the UK 2017.















School

Around 1
in 8 young
people
have been
bullied
on
social

media



3 in 4 parents have looked for or received information or advice about how to help their child manage online risks



Source: Ofcom (2017) Children and parents: media use and attitudes report



Source: Ofcom (2017) <u>Children</u> and Parents: Media Use and Attitudes Report (PDF)



Almost 1 in 4 young people have come across racist or hate messages online.







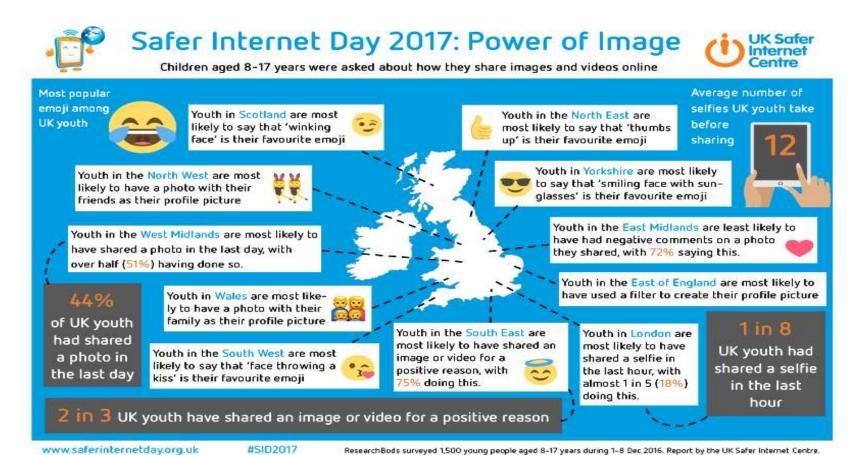








School















School



Picture Perfect



Average number of selfies young people take before posting one online



Average number of likes young people say they need to get on a photo before they feel happy



Nearly half of 8-17s (43%) worry about how attractive they look when they share photos online



Nearly half of 8-17s (45%) have used a filter to make themselves look better in the last year



www.saferinternetday.org.uk



ResearchBods interviewed 1,500 young people aged 8-17 years during 1-8 Dec 2016. Full report from the UK Safer Internet Centre: www.saferinternet.org.uk/power-of-image-research















Children and young people

- Well over 8 million children in the UK have access to the internet.¹⁰
- One in five children worldwide admits to doing things online their parents wouldn't approve of.¹¹
- Up to half of online adults worldwide and up to 40% of online children worldwide have made friends online.¹²
- In the UK, 43% of online adults and 26% of children enjoy their online relationships as much or more than their offline friendships.¹³
- In UK, adults believe that 4% of children have been approached online by a stranger. The actual per cent reported by UK online children is 20.¹⁴
- Most children will not report inappropriate internet contact to their parents because they are afraid of losing internet privileges.¹⁵













School

- 76% of 12-15 year olds have social networking sites higher in rural areas
- 91% of 5 15 year olds have access to the internet at home
- 50% of children have given their personal information to 'online friends' who they don't know in the 'real world'
- 24% of 9 16 year olds say they have seen sexual images in the last
 12 months
- 61% of young people receive spam gambling ads
- Most vulnerable groups for cyberbullying include children who are young carers, on free school meals, have an SEN statement, have less educated parents, parents who don't use the internet themselves, have disabled children in the family

Information from NSPCC (keeping children safe online)















How much illegal or inappropriate content is online?

It's difficult to know how much content is unsuitable for children on the internet but recent figures suggest that there's a lot out there:

- 9500 web pages were removed by the Internet Watch Foundation (IWF) worldwide in 2013
- 70,000 indecent images of children were reported to CEOP (Child Exploitation and Online Protection) in 2012
- 100s of pro-eating disorder websites are estimated to exist.













School

Parents Today.....

- Over half (56%) of 12 15s say they mostly use the internet alone
- 41% of parents of this age group say that their child has internet access in their bedroom
- Two in five (41%) of adults think content on the internet is regulated.
- 48% of parents think their child knows more about the internet then they do













School

Have young people changed?

Teens hang out, gossip, flirt, people watch, joke around, and jockey for status. These dynamics are at the heart of teen life... So they relish any opportunity to log in and engage with peers."

'It's Complicated' Danah Boyd

















Ways to chat online



Instant messaging



Web cam or video chat



Voice Over Internet Protocol



Chat rooms and forums

Chatting















School

How do offenders use the internet for child sexual abuse?



Games, social media and chat rooms enable people to make contact with children









Offenders can create multiple online identities and even pretend to be children and young people to trick real children into chatting and sharing.



Offenders can find out a lot about individual children before they make contact by looking at the things the child has posted online.



Offenders may target children who are particularly vulnerable or may contact lots of children in the hope that one will respond.



Once an offender has made contact with a child on a platform they can then very quickly move from these platforms to a private, un-moderated chat environment such as messaging or webcam.















Tactics used by offenders online

Offenders use a range of techniques to gain power and control over the young person. This power enables them to manipulate or coerce the young person into sexual activity. Online, this may include some or all of the following:

Gifts	Sexualised games		Leverage e.g. secrets		Blackmail
Flattery and compliments		Threats		Bribery	Mentoring

This process may involve building a relationship over time, or may happen very quickly, possibly within minutes.













School

Spotting manipulative tactics

```
IN-GAME PLAYER CHAT
[Eddie11]: Anyone know how 2 get onto level 14?
Dojo!!!!: Yehhhh
[Eddie11]: Please tell me... I've been stuck for ages @
[Jojo!!!]: Give me 100 coins and I will tell u
[Eddie11]: But then I won't have any left @
[Jojo!!!]: THEN U WILL NEVER EVER GET ON 2 LEVEL 14!!!
HAHAH
[Eddie11]: @@@
[Jojo!!!]: Trust me, it's worth 60 coins.
[jojo!!!]: I'll help you get more coins later...
[Jojo!!!]: I know this cool cheat for Level 14, it gives you a bonus
of 2000 coins!!!
[Eddie11]: WOAHHH!! Okay sending now.
                Eddie11 just sent 60 coins to Jojo!
[Eddie11]: So how do u get on level 14?
[Eddie11]: Hello??????
[Eddie11]: Tell me, I just gave you all my coins.
                  Jojo!!! Has left the conversation.
                                                         SUBMIT
```



















School

Impact of online sexual abuse

Non-contact abuse causes as much long term harm to a child or young person as contact sexual abuse:

Children forced, tricked or persuaded to participate in the abuse, for example by performing sexual acts on themselves, describe feeling as though they 'participated' in the abuse and did it to themselves. Children can feel they were to blame even though their actions were directed by the offender.



The existence of images can make it hard to feel that the abuse has come to an end and may be out there forever.



Offenders often tell young people that no one will believe them, or that if they tell anyone they will be the one in trouble















School

What is a 'nude selfie'?

There is no clear definition of 'sexting'. This module refers to 'nude selfies' which are self-produced naked or semi-naked images or videos of children and young people.

The guidance 'Sexting in schools and colleges: Responding to incidents and safeguarding young people' refers to 'youth produced sexual imagery' rather than 'sexting'.















The law

- Young people (under 18) who share sexual imagery of themselves, or their peers, are technically breaking the law.
- However, the National Police Chiefs Council (NPCC) is clear that we should not unnecessarily criminalise children and young people where they have consensually shared images of themselves.
- In January 2016 the Home Office launched a new outcome code (Outcome 21) in England and Wales. Outcome 21 states: "Further investigation, resulting from the crime report, which could provide evidence sufficient to support formal action being taken against the suspect is not in the public interest. This is a police decision."













School

Motivations

A young person might send a nude or nearly nude image or film for a variety of reasons, including:

As part of a trusting relationship.

For a joke.

To flirt.

For affirmation, such as positive feedback they receive from recipients.

Because they have been pressured, manipulated or coerced into doing so.













School

















The reality......

- As your child grows and becomes more independent, it is only natural that they take this independence online. In our teenage years we explore, try new things and sometimes push boundaries and take risks, this is an essential part of growing up.
- With all of the potential that the online world and new technology offers, young people now have access to huge opportunities. They use technology to express themselves, explore, and be creative; it has changed the way they communicate.
- The internet has changed all of our lives, and your child has grown up during this change. Many of the things that confuse, baffle or even scare us, are part of the everyday for them. For many of us, this can all be a bit too much.















Basic Recommendations for parents:

- **Be involved in your child's online life.** For many of today's young people there is no line between the online and offline worlds. Young people use the internet to socialise and grow and, just as you guide and support them offline, you should be there for them online too. Talk to them about what they're doing, if they know you understand they are more likely to approach you if they need support.
- Watch Thinkuknow films to learn more. The Thinkuknow programme has films and advice for children from five all the way to 16. Your child will see some of these at school, but they can also be a good tool for you to find out more about what young people do online and some of the potential risks.
- **Keep up-to-date with your child's development online.** Be inquisitive and interested in the new gadgets and sites that your child is using. It's important that as your child learns more, so do you.















- Set boundaries in the online world just as you would in the real world. Think about what they might see, what they share, who they talk to and how long they spend online. It is important to continue to discuss boundaries so that they evolve as your child's use of technology does.
- Know what connects to the internet and how. Nowadays even the TV connects to the internet. Your child will use all sorts of devices and gadgets; make sure you're aware of which ones can connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet is it your connection or a neighbour's Wifi? This will affect whether your safety settings are being applied.
- Consider the use of parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones. Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops.















- Emphasise that not everyone is who they say they are. Make sure your child knows never to meet up with someone they only know online. People might not always be who they say they are. There have been some high profile cases surrounding people who have claimed to be another young person online to lure potential victims. Locally there have been some investigations by the police into a grooming ring.
- You can't take back information that gets out on the internet. Make sure there are no images or comments that your children put onto the internet that you would not want to see. Once they have been uploaded and then downloaded they can't be taken back.
- **Know what to do if something goes wrong.** Just as in the offline world, you want to help your child when they need it. Therefore, it is important to know when and how to report any problem.















Most common social media sites in use in use are:

- Facebook
- Twitter
- What'sApp
- Ask.fm
- Instagram
- Snapchat
- Chat Roulette
- KiK messenger















CEOP Overview (Child Exploitation and Online Protection)

What does CEOP do?

- CEOP is a command of the National Crime Agency (NCA).
- CEOP is committed to tackling the sexual exploitation and abuse of children (CSEA), both online and offline.
- A multi-disciplinary child protection agency.
- Child-centred approach.









CEOP

A National

Crime Agency







- To identify, locate and protect children and young people from sexual exploitation and online abuse – both in the UK and globally
- To engage and empower children, young people, parent and the community through information and education
- To protect children and young people through the provision of specialist information and support to professionals, families, industry and community
- To enforce the law by bringing offenders to justice and acting to disrupt and deter future offending
- To enhance existing responses to the sexual exploitation and online abuse of children and young people by developing a safe by design online environment and refining the management of offenders







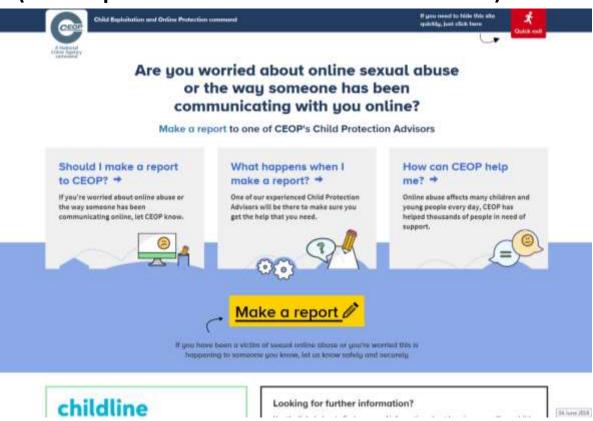








CEOP (Child Exploitation and Online Protection Centre)















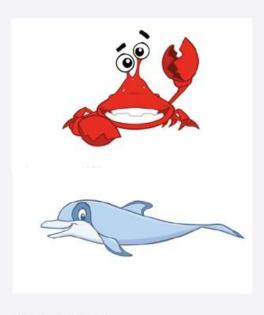
School

Thinkuknow resources for 5-7s





Lee and Kim's Adventures

















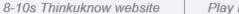
School

Thinkuknow resources for 8-10s



























School

Thinkuknow resources for 11-13s







11-13 Thinkuknow website



First to a Million







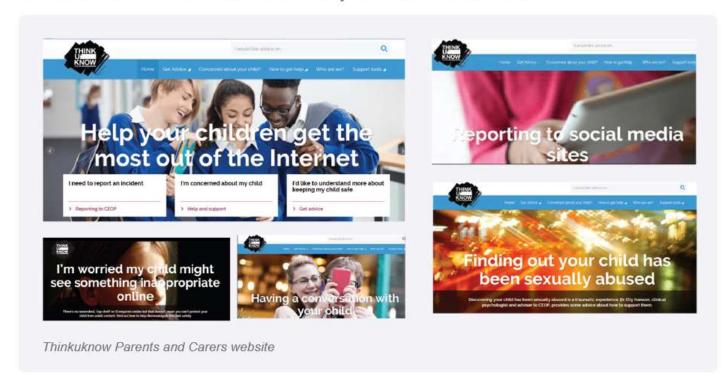








Thinkuknow resources for parents and carers









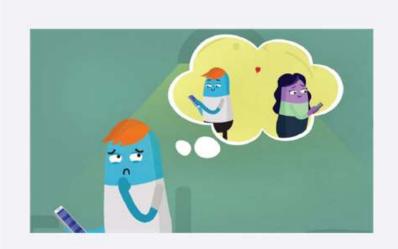








Thinkuknow resources for parents and carers



Nude Selfies: What Parents and Carers Need to Know



The World Changes. Children Don't.















CEOP (Child Exploitation and Online Protection Centre)

What is Thinkuknow?

The Thinkuknow programme aims to empower and protect children and young people from sexual abuse and exploitation through education.

Thinkuknow offers resources to cater for different age groups, audiences and needs:

5-7

8-10

educational needs and disabilities (SEND)

Resources for those with special

11-13

14+

Parents and Carers

























The Thinkuknow approach

"Today's children are growing up online, and make little distinction between life online and off. Their use of online games, apps and services plays a crucial role in the development of their identities, friendships, relationships, passions and aspirations. It is essential that we respond by offering them high-quality education based on the best available evidence."

Head of Education, CEOP





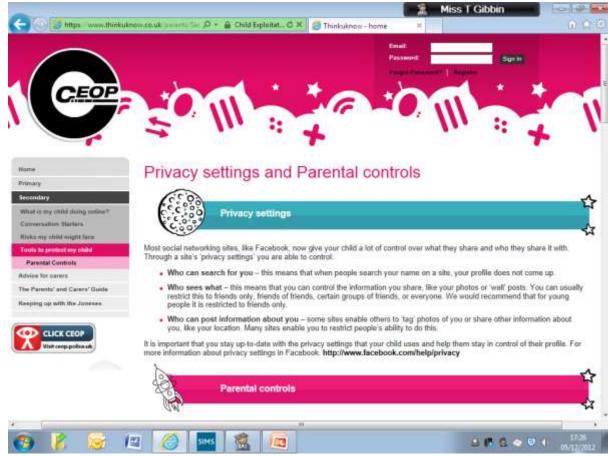








School

















CEOP's 3 Ps

<u>Prevent-</u> This includes the THINKUKNOW education programme to reduce vulnerabilities and promote safe behaviour online and offline. Intelligence and research drives the focus of the educational programme to keep pace with the shifting landscape of offender behaviour. CEOP also work internationally with partner agencies in countries where UK nationals pose a threat to children

<u>Pursue-</u> Pursue criminals and work with law enforcement colleagues throughout the UK and worldwide to bring them to justice. Keep pace with evolving technology, develop new tools and capabilities to assist CEOP and the National Crime Agency in tackling complex child abuse investigations in the online environment

<u>Protect-</u> Protect children by reducing the risk of them becoming victims, raise awareness of the threat posed by child sex offenders and ensure that expert child protection advice informs all decision making.













School

Virtual Global Taskforce (VGB)

24 hour presence both online and offline

 CEOP, America, Canada, Australia, Italy, UAE & Interpol

















eporting to CEOP



















What kind of concerns do people report to CEOP?

Reports from children and young people to CEOP have included:

Someone online has asked a child/young person to send them nude images.

A child/young person shared a nude image with someone online and then threatened/blackmailed as a result. A child/young person has or is planning to meet up with someone face-to-face that they have only met online.

Someone online is talking to a child/young person in a sexual way and making them feel uncomfortable.

Someone online is sending a child/young person pornography.

Someone online keeps asking a child/young person to go on webcam.















What happens when a report is made to CEOP?

When a report is made to CEOP:









The report will be read and risk assessed by a Child Protection Advisor at CEOP based on a Low/Medium/High rating. Where appropriate, the Child Protection Advisor will immediately start planning how they can help the child/young person.

The Child Protection Advisor will contact the person who made the report as quickly as they can. When they contact them, they will talk about what has happened, and will make a plan about what to do

The Child Protection Advisors' job is to make the child as safe as possible and so they may need to ask other professionals to help make sure the child is safe















School

Support and Report





















School

A wide range of CEOP videos can be found on You Tube as well as on the CEOP site

e.g. Consequences

e.g. Claire thought she knew......















Overarching Risks as Identified by CEOP:

- Unwanted contact/grooming
- Cyberbullying
- Harmful content/illegal materials
- Privacy/digital footprints















Mobile Technology Risks

- Images taken and uploaded at the click of a button may be breaking the law with regard to child protection
- Permanency
- Where they end up you do not have control over this
- Location-based services (e.g. geo-tagging)
- Unwanted contact
- Live Streaming















Tips for use of Mobile Technology:

- Don't enable your location or photo geo-tagging on your phone
- Only let friends you know in the real world have your phone number or location
- Think before you post
- Understand the safety functions and how to report















Tips for using social media:

- Privacy settings need to be set to "Friends only"
 - Including comments, posts and photos these settings need regularly checking for updates
- Use https: and strong passwords
- "Friends" should be people you know and trust in the real world
- Only post content and photos you wouldn't mind showing your family!
- Learn how to report any issues















Tips for using webcams:

- Never accept people you don't know and trust in the real world
- Giving out personal information can be risky
- Remember webcam feeds can be recorded and faked
- Don't webcam with people you don't know
- Turn the webcam off after use
- Delete people that make you feel uncomfortable
- Know how to report a problem
- We would recommend only allowing webcam use in the more public parts of the house – not when they are alone in their rooms















Online Gaming

- Top 10 online game operators in Asia earned over \$2bn last year
- Web games:
 - World of War Craft
 - Runescape
 - Everquest
 - Swordsman Online
 - Call of Duty
- Games consoles (Xbox 360, Playstation 3, Wii)















Risks of Online Gaming:

- Inappropriate content
- Unwanted contact
- Overuse / addiction
- Radicalisation
- Grooming















Tips in relation to Online Gaming:

- People are not always who they say they are online
- Keep gaming friends 'in-game'
- Don't give out personal information
- Learn the reporting processes in the game











Keswick School

 PEGI (The Pan-European Game Information age rating system) was established in 2003 to help European parents make informed choices













School





Violence - Game contains depictions of violence



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



Sex - Game depicts nudity and/or sexual behaviour or sexual references



Drugs - Game refers to or depicts the use of drugs



Fear - Game may be frightening or scary for young children



Bad Language - Game contains bad language















School

About PEGI?

What do the labels mean?

The PEGI labels appear on front and back of the packaging indicating one of the following age levels: 3, 7, 12, 16 and 18. 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.













PEGI 3

The content of games given this rating is considered suitable for all age groups. Some violence in a comical context (typically Bugs Bunny or Tom B. Jerry cartoon-like forms of violence) is acceptable. The child should not be able to associate the character on the acreen with real life characters, they should be totally fantasy. The game should not contain any sounds or pictures that are likely to scare or frighten young children. No bad language should be heard.



PEGI 7

Any game that would normally be rated at 3 but contains some possibly frightening scenes or sounds may be considered suitable in this category.



PEGI 12

Videogames that show violence of a slightly more graphic nature towards fantasy character and/or non graphic violence towards human-looking characters or recognisable animals, as well as videogames that show nudity of a slightly more graphic nature would fall in this age category. Any bed language in this category must be mild and fall short of sexual expletives.



instant as

This rating is applied once the depiction of violence (or sexual activity) reaches a stage that looks the same as would be expected in real life. More extreme bad language, the concept of the use of tobacco and drugs and the depiction of criminal activities can be content of games that are rated 16.



PEGI 18

The adult classification is applied when the level of violence reaches a stage where it becomes a depiction of gross violence and/or includes elements of specific types of violence. Gross violence is the most difficult to define since it can be very subjective in many cases, but in general terms it can be classed as the depictions of violence that would make the viewer feel a sense of revulsion.















Definition of cyberbullying:

'The use of digital technology (text messaging, email, social networking sites etc.) to bully, harass or abuse someone.'

What the bullies use:

Mobiles

Gaming

Forums

Social Networking sites

Sexting

Email















Cyberbullying traits

- It is an invasion of personal space for young people and is all encompassing and penetrating.
- The audience can be large, reached rapidly and can be unknown
- It is easier for perpetrators to remain anonymous through the online world or masquerade as another person
- The target of bullying can be anyone as physical and other factors do not come into play.
- Often young people who engage in cyberbullying get involved in an unintentional way.
- There is a disconnection as they are removed from the face to face.
- There is an evidence trail in the online world therefore there is the ability to track people















Privacy/digital footprint

- The information we put online leaves 'footprints'
- Young people can easily identified or traced
- Once information is online it is hard to remove it can be copied, cached etc. and may be around forever
- Information about individuals is not just stored on their profiles – friends, family contacts....















Parents need to become experts in offering age-appropriate advice and guidance to their children

Unwanted internet contact:

- Preventing online grooming and explaining to children how to report instances and remove any damaging content.
- Cyber bullying how to avoid, prevent, and deal with instances of cyber bullying, and how to report and remove offensive material created as a result of cyber bullying.

Inappropriate internet content:

- How to avoid, report and delete content which may be: pornographic, illegal, obscene, violent or likely to incite racial or religious hatred.
- How to avoid and report content which encourages illegal or dangerous activity by pupils, or is simply age-inappropriate.
- How to set a good example with regard to downloading software safely, avoiding viruses, adhering to copyright law etc.













Parents need to become experts in offering age-appropriate advice and guidance to their children (cont.)

Privacy:

- How to ensure social networking content stays private and doesn't end up in search results years later.
- How to ensure passwords are strong, password-protected information, such as banking details or parental online shopping details remain safe.
- How to prevent and deal with junk mail and spam, and also how to spot internet scams and 'phishing' emails and messages.
- Understanding how websites store and track data which might be used for valid marketing reasons, or abused to create spam or facilitate identity theft.

Mobile phones and devices:

 Understanding how difficult it is to remove tracking data from mobile phones and how important it is to safeguard privacy on mobile devices – more so than on laptops or PCs.













School



www.parentinfo.org





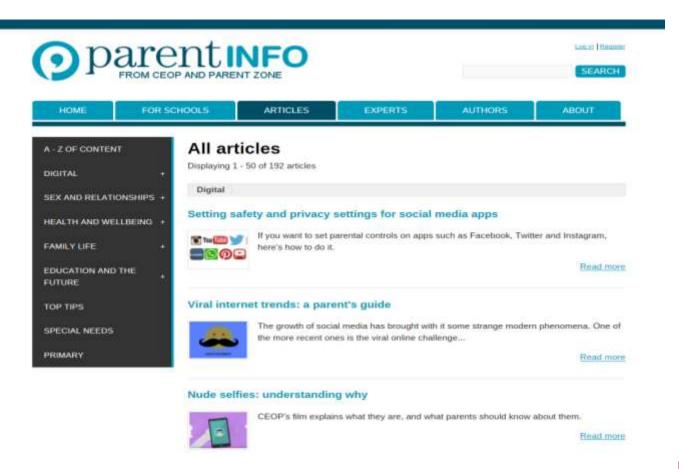








School















School

What is - and isn't - legal online?



The digital world is so new that half the time we don't know what the rules are. In fact, there are plenty of laws governing what you can and can't do online. Here's our guide to what you should and shouldn't be doing online (legally, anyway).

Read more

A parent's guide to Kik Messenger



What adults need to know about the app their children love using.

Read more

WhatsApp: a guide for parents and carers



Teenagers love WhatsApp - as do a lot of parents. Here's what you need to know about it...

Read more

A parent's guide to Vlogging - what you need to know



Know your Zoellas from your PewDiePies: a parent's guide to vlogging.

Read more

Don't pay the price for your child's online fun



Parents sometimes end up paying unexpectedly large phone bills and don't know why. PhonepayPlus, the premium rate services regulator, explains what to look out for when giving your child a mobile device...















The NSPCC have a great deal of excellent information and advice

Online abuse More on this topic What is online abuse Online abuse is any type of abuse that happens on the web. Worried whether through social networks, playing online games or using mobile phones. Children and young people may about a experience cyberbullying, grooming, sexual abuse, sexual child? exploitation or emotional abuse. Contact our trained Children can be at risk of online abuse from people they know, helpline counsellors for as well as from strangers. Online abuse may be part of abuse 24/7 help, advice and that is taking place in the real world (for example bullying or support. grooming). Or it may be that the abuse only happens online (for example persuading children to take part in sexual activity help@nspcc.org.u online). 0808 800 Children can feel like there is no escape from online abuse -5000 abusers can contact them at any time of the day or night, the













School

Digital parenting – advice published by Vodafone



My Tech Family









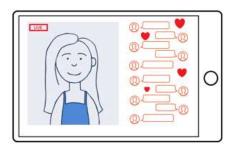






School







Live Streaming: Information for parents and carers





















What is live streaming?

- Visual broadcast live over the internet via any smart phone or tablet with a camera
- Live streamed videos are unedited and shared without delay
- Unmoderated, unrehearsed & unpredictable
- Viewers can send gifts, comment and talk directly with the person live streaming



















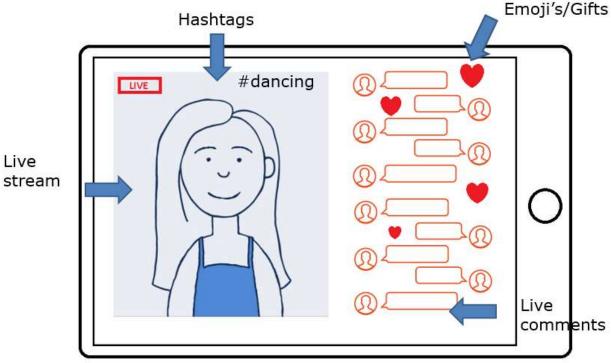






Live

What does it look like?



















Popularity

Live streaming is highly appealing to children and young people as it offers the opportunity for them to be a creator and presenter and be seen by a potentially huge audience.



Live.me: Over 20,000,000 downloads



YouNow: 10,000,000 - 50,000,000 downloads



Live.ly: 5,000,000 - 10,000,000 downloads



Periscope: 10,000,000 - 50,000,000 downloads



Musical.ly: 100,000,000 - 500,000,000 downloads











^{*} References: Google Play October 2017. All referenced have an age limit of 13+ years



School



What can you do?

- Ongoing conversations with your child about their internet use
- Children should only live stream in public rooms
- Look out for children moving to private platforms
- Build resilience, particularly where children are feeling lonely
- Encourage children to identify safe and trusted adults
- Make sure children know where to go for support



















Thinkuknow website for parents/carers















