The digital generation

October 2017
Compiled by Enough Abuse for IAPS
The Digital Generation

LATEST CRAZE Sept 2017- children “going live” on you tube and other social media
“The most important question you ask children is “Do you REALLY know with whom you are communicating?” (February 2012 – DI Kay Wallace West Midlands Police Chief for Online Safety Team)

New version 2017 CASTLE CLASH online game being accessed by PAEDOPHILES: With over 100 million players worldwide, you hire powerful Heroes to lead your army of mythical creatures. Fight your way to become the world’s greatest warlord. Put your strategies to the test in dungeons, raids, and more! Now available in French, German, Spanish, Italian, Russian, Japanese, and Korean.

Met police warning – 29th JULY 2017 – money mules - young people aged 13 and younger are being offered money to use their accounts to transfer money through the bank accounts as a money mule and this is has doubled in the last year through social media and at school gates

INSTAGRAM – RSPH – royal society of psychological health states INSTAGRAM – is the worst social media platform for harming the mental health of young people. 20th MAY 2017

MUSICAL.LY – age limit of 13 yrs old and heavily infiltrated by paedophiles seeking dance videos

New app for parents – Gallery Guardian

Parents worried their children are swapping inappropriate pictures and selfies with friends or even strangers online are being offered a smartphone app to automatically spot suspect images.

The firm behind Gallery Guardian says it uses sophisticated image recognition software to scan pictures appearing on a child’s mobile to detect naked skin, genitalia or breast exposure. If the app spots a suspect image on the child’s phone, the parent is immediately sent an alert reading “suspicious image detected”. (source – the Telegraph)

News: 22 April 2017:

The Blue Whale Challenge: This is a Russian forum app it is NOT A HOAX, people make contact who wish to die and an administrator talks you through how to take your own like It is vk.com – Russian name is vkontakte (source INEQE)

Online Abuse Definition: The repetitive use of digital technology with intent to cause harm. Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones. Children and young people may experience cyberbullying, grooming, sexual abuse, sexual exploitation or emotional abuse. (Source NSPCC)

The Law:
Whoever signs the contract for the mobile phone and internet contract is LEGALLY responsible for the communication traffic, with messages and images and photos

**As of 3rd April 2017 a new law** will be in place leading to a 2 year conviction for those adult groomers sexually communicating with children – off and on line

**QUESTIONS YOU SHOULD ASK and ASPECTS TO CONSIDER**

- Do you know the current top 5 social media platforms your pupils, child and friends use?
- Is your on line safeguarding in school contemporary, credible and relevant regarding social media?
- Do you know the moderate and significant risk indicators of issues online shown in behaviours?
- Do you ask why a child keeps their mobile face down and leaves a room as soon as a message arrives?
- Do you know where and who to go to for assistance BEFORE a crisis happens?
- The CONTEXT of a child’s life is KEY to understanding and reflected in how they access social media
- Do you see the internet as virtual or accept is it the REAL world for youngsters as is the harm caused?
- Pupil behaviour online is MORE important than ANY school e- safety policy!
- SEN pupils are 16 % more likely to be bullied online
- ChildLine receive more calls about bullying than any other, and children as young as 6 are now calling them
- Be **strident** in obtaining the help you need THE CHILD IS KEY
- Virtual abuse will NEVER go away and causes abject panic when the child realises
- THE LAW should change and DECRIMINALISING sexting for youngsters under 16 and allowing to see it as an error of judgement to encourage them to disclose so police can track and remove the images asap AND GIVE THEM HOPE
- Children like to be liked and seen to be liked which creates a vulnerability. Rapport leads to friendship which leads to sharing images etc
- The game **Grand Theft Auto** encourages sexism and criminal violence
- Do you know the benefit of DECOY APPS?
- Do you operate a safety settings audit?
- Do you check your child’s digital footprint?

**HMC report May 2017:**

The survey - conducted via a mixed state and independent academy chain – reveals:

- Children’s biggest concern about being on-line is lack of sleep (47%) but only 19% of parents chose that as their biggest concern about their children.
Parents’ biggest concern about their children being online is the impact on their social skills (32%) but only 10% of young people chose this about themselves. Addiction was the next biggest worry (26%) amongst parents with lack of sleep third.

Over a third of children thought parents’ biggest concern about their children’s device use would be lack of sleep (34%).

72% of students said they spent anything between 3 and 10 hours online on an average day during weekends and holidays. 11% said they were online during weekends and holidays between 10 and 15 hours a day. However, nearly half of students said they “wouldn’t mind” if all their devices were taken away for a weekend. Another 20% said they would feel ‘isolated’ and 11% would feel ‘panicky’.

Over a third (36%) of children people say they have asked their parents to stop checking their mobile devices. Almost half of them (46%) say it makes no difference when they do so. However, under 10% of parents thought their time spent on devices was concerning their children.

22% of students felt that the use of mobile devices stopped their families from enjoying each other’s company and 82% of children say meal times should be device-free.

95% of parents reported that they do not use mobile devices at meal-times (but 14% of children said their parents were on-line at meal-times and 42.44% of them felt ignored or annoyed by it).

43% of parents thought they spent too much of their own time online. 21% of parents report being online for 6-10 hours during an average working day and 37% say they are online between 3 and 5 hours a day at weekends. 5% are online between ten and 15 hours at weekends.

72% of students said they spent anything between 3 and 10 hours on-line on an average day during weekends and holidays. 11% are online between 10 and 15 hours a day and 3% say they are online 16-20 hours a day during those periods.

However, the majority of children don’t think their parents are concerned about the amount of time their children spend on mobile devices. 56% answered no to that question.

Cyber Bullying and Cyber Stalking:

Cyber Bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature EVERY 30 MINUTES EVERY DAY A CHILD SELF HARMS DUE TO CYBER BULLYING

90% of children state they wouldn’t tell their parents and 1 in 3 children report suffering as victims of cyber bullying (Source - Marie Collins Foundation). This presents a very real danger as children have taken their own lives in desperation to escape this cruelty. The bullying is set to cause distress.
- 1 in 3 children have experienced cyber bullying which overlaps into the playground
- 1 in 13 suffer persistent bullying causing them to self harm and possibly commit suicide
- 50% of adolescents and teen have been bullied online and the same % and category have engaged in bullying online (Univ of Beds)
- 44% of child suicides had bullying as part of the cause and poor achievement at school (Source of above – Marie Collins Foundation)
- In an American survey, of the children who admitted they had been bullied, 87% said it had happened on Facebook, 19% on Twitter and 13% on BlackBerry Messenger (Source Guardchild.com)
- In a American survey of random middle and high school children (aged 11 to 18) the below results were found:
  - Overall, about 25% of the students said that they have been cyber bullied at some point in their lifetimes
  - About 9% said they were cyber bullied in the 30 days preceding the survey
  - Similarly, about 16% of those who we surveyed admitted that they had cyber bullied others at some point in their lifetimes (about 6% in the most recent 30 days)
  - In 2014 a review of all research conducted by the Cyber bullying Research Centre concluded that about one out of every four teens has experienced cyber bullying, and about one out of every six teens has done it to others.

- A couple of other broad generalisations can be made about cyber bullying, based on recent research:
  - Adolescent girls are just as likely, if not more likely than boys to experience cyber bullying (as a victim and offender)
  - Cyber bullying is related to low self-esteem, suicidal ideation, anger, frustration, and a variety of other emotional and psychological problems
  - Cyber bullying is related to other issues in the ‘real world’ including school problems, anti-social behavior, substance use, and delinquency
  - Traditional bullying is still more common than cyber bullying
  - Traditional bullying and cyber bullying are closely related: those who are bullied at school are bullied online and those who bully at school bully online (Source of the above – Cyberbullying.org)
- “Porn revenge” is a form of cyber bullying, where the perpetrator threatens to send images and blackmails the victim
- Cyber Stalking is where an offender is totally fixated on their victim and can lead to violence, even death

**CPS New Policy as of 10th December 2012:**
In a case of cyber bullying, evidence of the first 3 points will bring a prosecution:
1. A credible threat of violence against a person or property
2. Is the bullying at a specific target
3. Breaching a court order?
4. Freedom of expression means it is no longer an offence to say bad things about someone.

Explain to the children – there are consequences to taking part in cyber bullying, emphasis real people are receiving the texts, it’s not a joke and needs to be taken very seriously!

**Academic Impact of Online Games:**

- A 20 year old man died after 12 hour gaming sessions. The Xbox gaming enthusiast suffered a blockage to his lungs when he developed deep vein thrombosis. *(Source – Mail Online).* Internet addiction is increasing

- Research from Cambridge University suggests that 14-year-olds who spend an hour a day on screens during their leisure time score nine fewer points at GCSE when the sum of their grades is calculated – the equivalent of dropping two grades from a B to a D. Two extra hours results in 18 fewer points at GCSE *(Source - The Guardian)*

- Children who spend more than three hours a day on social media websites are twice as likely to suffer mental health issues, official data suggests. A report from the Office for National Statistics (ONS) found higher levels of emotional problems, issues with other children, hyperactivity and poor behavior among youngsters who spent a lot of time on social media websites *(Source – Mirror.co.uk)*

**Advice Regarding School Websites and Literature:**

The UK Safer Internet Centre website holds best practice policies for teachers, head teachers, governors and others about the safe use of technology. Or you can call the professionals online safety helpline (which is on the UK Safer Internet Centre page) for any further advice about best practice policies in this area.

The UK Council for Child Internet safety has proposed far more robust systems are needed, involving the use of digital “age” tokens. This is as a result of a father suing Facebook for not doing enough to protect his 11 year old from opening an account and contacting men.

For best practice regarding pupil safety - mobile phones, iPads and tablets should not be permitted within the school working day environment.

**Ofsted Report - Online Safety in Schools - July 2015:**

- Governors are the consistent weak link, and showed little convincing evidence of having a good grip on school practice, and not making much strategic input to current school practice, together with their own lack of awareness

- Over 25% of students cannot recall if they had been taught about online safety in last 12 months

- 25% of students lacked confidence in their teachers’ knowledge of online safety issues

- 5% of schools do not have an online safety policy

- Staff training is inconsistent and what SML – Senior Management Leaders, see as training is not reflected by staff. Emergency training is delivered if there is an incident
• Reporting is generally poorly understood and inconsistent many schools lack clear approaches, leaving students unsure.

**Age Limits:**
- Facebook, Instagram, Twitter; Tumblr, Reddit, Secret, Snapchat, Pinterest, Habbo, Google+ – AGE LIMIT 13 YEARS OLD
- Linked in – AGE LIMIT 14 YEARS OLD
- What’s App – AGE LIMIT 16 YEARS OLD
- Vine – AGE LIMIT 17 YEARS OLD
- You tube, Wechat, Kik, Keek, Foursquare, Flickr - AGE LIMIT 18 YEARS OLD, but 13 to 17 years old with Parental permission.

*50% of parents are unaware of the social media age limits and 1 in 5 parents did know there WERE any social media age limits* (source 17th March 2017 NSPCC)

It is illegal for an underage child to use one of these sites so if you know a child that is you can report it to the site involved, such as Facebook, Instagram, Snapchat etc. Parents need to be closely monitoring their child’s Internet use to ensure this does not happen. Parents should also read the terms and conditions set out for various apps and games

**Trauma of youngsters watching pornographic images and videos:**
- 2 clicks of a mouse allows easy access to the most bizarre and sadistic images
- Easy access to these images is causing “acting out” behaviours
- 70% of porn videos show misogynistic acts within the first 2 minutes – which in turn feeds youngsters minds to normalise this behaviour *(Source - Peer Support)*
- 1. Raises trauma / cortisol levels 2. Desensitises them 3. Perceived as “normal” behaviour *(Source - Peer Support)*
- ChildLine have seen a 70% increase in BOYS distressed by porn they have seen

**Online Victims:**
- CEOP receives 1000 reports of online abuse a month
- Children who feel unattractive can and do feel highly attractive online
- Tend to be middle class girls from good homes and schools. Many more girls are victims of on line abuse than boys
  When asked why they became involved in the online activity, girls said, “Something was missing in my life.” They feel online is cosy, fun; they gain attention and had affirmation they look and are OK. These girls feel insecure and lonely *(Source of all above - Marie Collins Foundation)*
- Removing a mobile phone or devices from a child raises anxiety more than if you lost your keys and wallet, this is their world now
- Even if children do not have a phone or a device they will share others who have

**Online Sex offenders:**
- Only 1 in 14 arrested for viewing child images are convicted
- Very few have any previous convictions or any criminal record
• Often have competent IT skills and high IQ – often in excess of 120
• They admit to “fishing trips” – trawling to see who is online and keep going until they gain a response
• Conversation becomes immediately sexualised
• Many have as many as 9 different ID’s and keep a log so they know to whom they have spoken and what has been said (Source - Jonathan Taylor Social Media & Online Safety Consultant)
• Beware of those using numbers/avatars in their email address/games username such as “js1979@hotmail or “john49@hotmail” – the number is a clue - often the person’s age or year of birth and may indicate they’re not a child
• Abusers copy images from Facebook, steal ID’s and use them as they please. They will use friends on Facebook sites to access the images. Many passwords are easy to crack. It is easy for an abuser to track down victims through online messages and photos, for example “happy 16th” will indicate the age of the person on the page
• “Flirty” email addresses such as “sexy kitten,” “hot lips,” “party lass” etc. are an invitation flag to an abuser and suggest a type of lifestyle and risk taker. It is inadvisable to use sexualised names
• CATFISHING – adults who pretend to be children to lure them in on the internet

Photography and phones:
• This is the first generation where most people have a camera in their pocket. Unknowingly a photo can be taken on an iPhone and with face recognition on the Internet it will find the Facebook site of the individual where all personal details can be easily hacked and the victim stalked
• Safe Images: The Granny Test. If you wouldn’t show your Mum, Granny or Aunt don’t display it on a SMS
• Paedophiles: photo shop for images to cut and paste and out into the dark web

Statistics (source: Saturday telegraph – 23 September 2017)
• 9% of 11 to 15 year olds are communicating via social media at 10pm
• 42% of 8 to 11 year olds prefer watching You Tube to watching a TV set
• 51% of 12 to 15 year olds use Snap Chat
• 32% of 8 to 11 year olds have a smart phone
• 17% of 12 to 15 year olds have deleted their browser history
• 34% of 12 to 15 year olds have encountered “hate speech” on online in last year
• 21% of 12 to 15 year olds play games with people they have never met
• 64% of 12 to 15 year olds have a good balance between screen time doing other things
• 41% of parents admit they find it hard to control their child’s screen use
• 72% of 12 to 15 year olds have a social media profile

**What Are Decoy Apps?**
As its name suggests, a decoy app is a mobile application designed for misdirection. It presents itself as one thing, while it does another.

And the thing that decoy apps generally do is hide stuff. Like...

- Text or “sext” messages to illicit sexual partners
- Photos containing shots of you with people you shouldn’t necessarily be with – like lovers who are cheating on one or more of their respective partners
- Call logs and contacts that could be traced back to people or organizations you shouldn’t be seeing or dealing with
- Porn

**How Do Decoy Apps Work?**
A decoy app will generally provide tools for the creation of one or more hidden folders or “vaults” in the storage area of your mobile device. Files and data that you wish to conceal may be copied over to these secret stashes – often with the option to encrypt them, before the move. Once you delete the files from their original location, another user looking at your device won’t see the hidden folders (with their encrypted copies) in any directory or gallery listings.

The decoy app itself can’t be accessed without the security code or password you specify – and there may be options to set a “burner” or emergency password you can key in to erase all traces of the vault in extreme circumstances, or a code that simply leads to an innocuous front (like a folder of dummy images). Most importantly of all, the actual user interface of the decoy program masquerades behind the facade of another breed of software entirely.

Though several variants exist, some of the more popular ones include:

- “SpyCalc” or “Smart Hide Calculator” apps, which present as a functional calculator, currency converter, or similar – but if you enter your pass code from its numeric pad, the calculator’s face gives way to the decoy app’s hidden folders management system.
- “Audio Manager” type apps, which on the surface provide a functioning set of volume and sound controls for your device – but if you press on a given area of the screen, they’ll dissolve into the app’s vault manager.
- “Best Secret Folder” variants, which take the form of a normal-looking (often empty) folder – but with a specially configured set of moves (tap a certain screen area, or enter a PIN code), the app gives access to a secret vault where you can hide apps you don’t want to be seen in launchers or your app drawer.

**Why Use Decoy Apps?**
Okay, here’s a confession: We pulled a bit of a decoy, in the preamble to this article.

While it’s certainly true that this type of app can be legitimately used to hide corporate data or intellectual property from prying eyes, the reality of the matter is that decoy apps are typically deployed for much less noble purposes. Like...

- Hiding the call, text, or email evidence of unsanctioned personal or business relationships
- Hiding documentary, photographic, or video evidence tying the device owner to individuals, organizations, or locations (physical or virtual) they shouldn’t legitimately be in personal or business contact with
- Concealing illicit, pornographic, inflammatory, or otherwise sensitive material (including hate speech and the like) which might expose a device owner to criminal prosecution, religious or social persecution, or forms of exclusion
- Concealing mobile apps that are being used to engage in offensive, dangerous, or illicit activities (and may involve any of the reasons outlined above)

Who’s Using Decoy Apps?
There’s anecdotal and forensic evidence to suggest that decoy apps are being employed by a wide range of users, representing different genders, age groups, social sectors, and motivations. Among these are:

- Men and women using decoy apps to hide evidence that they’re cheating on their partners
- Students at a U.S. high school (in Cañon City, Colorado) setting up an illicit ring for sharing nude and lewd photographs
- Kids using decoy apps to hide text messages, call histories, documents, application use, and browsing activities from their parents
- School students using the apps to hide messages and files used in waging cyber-bullying campaigns against their peers
- Decoy apps may be making it easier for stalkers and sexual predators to plan and stage harassment campaigns, and to share images and videos with like-minded individuals
- Criminal gangs are probably using decoy apps to facilitate illegal transactions (including drug deals, extortion, and theft), and to hide incriminating evidence from the eyes of local and regional authorities
- Cyber-criminals may be using decoy apps to share intelligence, and/or to facilitate any number of different kinds of attack
- There’s the very real possibility that terrorist networks and militia groups may be using decoy apps in a similar manner, or as a vehicle for waging hate campaigns and digital harassment

How Bad Is It?
For a 2015 interview, private investigator and computer forensic examiner Robert Namowicz of Spindletop Investigations compiled a list (which ran to 14 pages) of decoy apps
readily accessible from mobile app stores – and that was just the apps he was capable of hacking into, himself.

In that same year, the Private Photo Vault decoy app was the 28th most downloaded photo and video app on the App Store, as determined by the mobile application measurement service App Annie.

And decoy apps have been increasing in availability and complexity, ever since. According to technology journalist and former detective Cindy Murphy, these apps are introducing a whole new level of complexity into the work of digital forensic investigators.

**Some Recommendations for Parents**

For parents concerned about what their children are getting up to within the hidden recesses of their own machines, there are several recommendations:

The iOS ecosystem provides some protection in the form of its “Ask to Buy” controls, which allow parents to screen mobile apps before they’re downloaded to their children’s iPhones. Configuration procedures (which require activation of Family Sharing) are available on the Apple website.

Similar parental vetting procedures may be set up at Google’s Play Store, with rules governing the maturity level at which children may be permitted to download and install certain apps.

**Sextortion:**

**Definition** - Sextortion is basically a type of extortion with a twist. Instead of extorting money or material goods from a victim, a sextortionist will extract sexual favours from the victim by using intimidation, fear, and blackmail. The likely victims of this new type of exploitation are teens since they possess many if not all of the risk factors associated with it.

Because of technology like the use of mobile phones and internet, they go as far as taking photos of themselves naked or showing a part of their body using a camera or phone and then uploading them to the web. This also often goes on without the parents being aware. Sometimes even under their own roof. On top of this, there are an unknown number of online predators and sex offenders out there that surf the web to find potential victims.

What happens next is unfortunate. When a sextortionist (who is usually a sex offender) grabs any photo of a teen naked or anything that shows sensuality, he uses this as a weapon for blackmail. He then finds a way to contact or reach the teen in the photo and then tells her to send more images or videos or else he will tell everyone about her secret. She is left with no choice but to send more material just for the sextortionist to refrain from placing her under a cloud of embarrassment and shame

**‘Sexting’:**
**Definition:** 'Sexting' is the exchange of self-generated sexually explicit images, through mobile picture messages or webcams over the Internet *(Source – NSPCC)*

“Cat fishing” duped into intimately interacting with men and women on web cams then blackmailed. Currently used by those pretending to be football agents with many football academy youngsters and blackmailed to pay £50k plus to stop images being released onto the Internet *(source: The Guardian 29th July 2017)*

**Tackling sexting**

The NSPCC offers advice to professionals about how to respond to incidents of sexting. This include: writing a sexting policy and procedures; what to do if a young person makes a disclosure about sexting; increasing public and professional awareness of issues surrounding sexting.

**Source:** NSPCC **Date:** 27 September 2016

- Statistics from the children’s charity Beat Bullying study on young people (12 – 15) found the below:
  - Over one third (38%) had received a sexually explicit text or email – 36% of males and 39% of females
  - Over a quarter (25%) had received an offensive sexual image
  - 85% knew the identity of the aggressor
  - The majority were peers and only 2% indicated that it was an adult
  - Just under a third (29%) have been chatting online when someone started to talk to them about sexual things
  - 6% had received a message or image on the subject of sex which subsequently made them feel uncomfortable or upset
  - Over half of teachers (54%) were aware of pupils creating and sharing sexually explicit messages and images via the Internet or mobile *(Source of above – ParentsProtect.co.uk)*
  - Most young people do not see 'sexting' as a problem and are reluctant to talk to adults about it because they are afraid of being judged or having their phones taken away
  - There were over 1,200 ChildLine counseling sessions with young people that mentioned 'sexting' in 2014/15 *(Source of above – NSPCC)*
  - Many girls receive 20 to 30 ‘sexting’ messages a day for sex. Many boys think ‘sexting’ bigs them up and makes them appear to be macho *(Source - Marie Collins Foundation)*
  - Many boys use tactics to show ownership of a girl to their mates, for example a boy may suggest the girl writes the boys name on her breasts which he photographs shares online
  - Children as young as 11 and 12 are ‘sexting’
  - In July 2015, the Daily Mail carried the story of 13-year-old Sophie who sent a topless picture to her boyfriend and she said:

"It's just normal," she said. "If a boy likes a girl, the first thing he does is ask for your
picture. Some of my friends had done exactly the same thing for boys. It's just that theirs didn't get sent around. As soon as I arrived at school, I knew most people had seen it because they were staring and laughing. When my back was turned, I heard the words slag and slut. I tried to ignore it." (Source – Huffington Post.co.uk)

‘Doxing’

**Definition: “Doxing”** is the process of retrieving, hacking and publishing other people’s information such as names, addresses, phone numbers and credit card details.

**NOTE:** The taking of indecent images and nudity even between consenting adults and used for sexting is against the law!

**New report’s reveals children at risk of exploitation online:**

**Organised crime online**

Europol has published its Internet organised crime threat assessment (IOCTA) for 2016. Key findings include: while peer-to-peer networks are still a popular platform for the exchange of child sexual exploitation material (CSEM), there is an increase in the volume of material being exchanged on the Darknet; the use of end-to-end encrypted platforms for sharing media, along with anonymous payment systems, has contributed to an increase in the live streaming of child abuse.

**Source:** Europol  **Date:** 28 September 2016

Almost half of young people (48 per cent) living at home say their parents only know some of what they do online, according to an Ipsos MORI poll commissioned by Barnardo’s. One in 9 (11 per cent) surveyed for the children’s charity admitted their parents understood nothing about their online activity. Also, a third of young people (33 per cent) questioned say they find it easier to show their real personality on the Internet than with people face-to-face.

The findings coincide with a new report, ‘Digital Dangers’ jointly published by Barnardo’s and the Marie Collins Foundation. It says all children are vulnerable to being groomed and sexually exploited on the Internet via mobile technology.

For the report, 34 project workers from 11 Barnardo’s specialist child sexual exploitation services throughout the UK were interviewed about the young people they support. Barnardo’s workers reported that those who were at risk, or were victims of sexual exploitation online often:

- Consider it normal to use sexualised language and send naked photos of themselves to strangers online
- Keep online grooming or abuse a secret
• Do not fit the stereotypical vulnerable or ‘at risk’ child profile and could be in any family
• Can be younger than those children sexually exploited and groomed offline.

The report also found that professionals and parents lack technology expertise to check online behaviour. Barnardo’s chief executive Javed Khan, said: “As a father of four children I am concerned about the dangers facing them and other children online. As parents, we must all try to better understand the mobile technology they use and what they are using it for, to help keep them safe. We want Governments across the UK, industry and voluntary sector to implement measures to prevent sexual abuse and exploitation happening online, along with ensuring children get vital sex and relationship advice to help them be more aware of the risks they are taking online.”

Digital Dangers, author Tink Palmer, Chief Executive of the Marie Collins Foundation said: “Children are being targeted by perpetrators through their smart phones and other mobile devices. Technology has made them easier targets for abusers, who take advantage of their relative naivety. If parents/carers are worried about changes in their children’s emotional wellbeing, one of the first questions they should ask is, ‘what is happening online’? A greater emphasis needs to be given to training professionals working in the police, social work, health, education and voluntary sector so they can better protect children from online abuse.”

In 2004 half (52 per cent) of 7 to 16 year old owned a mobile phone. According to Ofcom this has increased, with 65 per cent of 12 to 15 year old’s now owning a smart phone and 20 per cent of 8 to 11 year olds (Source – Barnardos)

**What’s The Right Age?**
(Source NSPCC Online)

• Many social networks have a minimum age of 13 (because of laws governing their use in the USA, where the majority are based)
• Children become more interested in social networks when they start secondary school
• At the age of 11, they're becoming more independent and want to be part of the social network of their new school – whether online or in person
• 50% of all 11 and 12 year-olds in the UK use a social networking site, according to our research. This is because it's easy for children to access sites intended for older users
• Social networking accounts can also be used to access a range of other sites – just think of all the websites that invite you to 'Sign in using Facebook or Twitter’
• Some parents may think it's OK for their 11-year-old to use a site aimed at over 13s, but it’s worth bearing in mind that it’s not just that site's content you need to think about
• 7 in 10 of 12-15 year olds who go online have a social network profile
• 1 in 5 of 8-11 year olds who go online have a social network profile
• 1 in 20 of 5-7 year olds who go online have a social network profile
**Online Child Abuse Images:**

In 2016 IWF has 57,335 reports confirmed of CSA URL’s

Europe now hosts 60% of CSA webpages *(Source IWF - 3 April 2017)*

Child sexual abuse content increasingly being ‘masked’ online to hide crimes – latest global data – *(Source IWF – 3 April 2017)*

The “disguised website” technique makes detection harder.

Criminals are increasingly using masking techniques to hide child sexual abuse images and videos on the internet and leaving clues to paedophiles so they can find it.

The Internet Watch Foundation (IWF) will publish its latest global trends and analysis in its Annual Report 2016 on 3 April.

It shows that a technique they first identified in 2011 is being more widely adopted by criminals making detection and removal of child sexual abuse images and videos from the internet, harder.

IWF has identified commercial child sexual abuse websites which only display the criminal imagery when accessed by a “digital pathway” of links from other websites. The pathway is like a trail of breadcrumbs; when the pathway is not followed or the website is accessed directly through a browser, legal content is displayed. This means it’s more difficult to find and investigate the illegal imagery. It also means that criminal enterprises online are receiving legitimate banking services, as checking their website won’t automatically reveal the criminal content.

When IWF first identified this technique, they developed a way of revealing the illegal imagery, meaning they could remove it, and the websites could be investigated. But the criminals continually change how they hide the illegal imagery, so IWF’s expert analysts adapt in response.

In 2016, 1,572 websites were found to be using this method to hide child sexual abuse imagery. This is an increase of 112% on the 743 disguised websites identified in 2015.

- It is difficult to estimate the number of websites globally that depict child abuse images. The Internet Watch Foundation (IWF) has identified and taken action against some 16,700 instances of child sexual abuse content on different web pages worldwide in 2010, compared with identifying around 10,600 URLs of individual web pages or websites in 2006
- Most significantly, however, child abuse images are increasingly shared among networks of like-minded individuals through peer-to-peer distribution, which avoids the necessity of housing the images on storage systems owned by third-parties such as Internet service providers
- There are millions of child abuse images on the internet, with tens of thousands of individual children depicted in the images
In April 2010, the NSPCC published a study in which media reports of court cases in England and Wales between April and September 2010 were analysed. The NSPCC found that close to 3 million images had been circulated by 284 offenders who were consequently convicted. Some 35,000 images were classed as categories 4 and 5, which are the most severe levels of abusive images (England and Wales) in 2002.

Once on the Internet, images can easily be transmitted to other websites, downloaded onto mobile phones or distributed to an unknown number of recipients via email without the knowledge or consent of the individual depicted.

Perpetrators can also sell children for live abuse online, in which the perpetrators announce to their online ‘peer’ or ‘peer group’ their intention to abuse a child on a set date and time. Those who wish to watch the live abuse arrange with the perpetrator to be online at that time.

Recent evidence from the European Financial Coalition against Commercial Sexual Exploitation of Children Online indicates that organizers of commercial child abuse websites distribute images but do not produce them. Not all distributors are from organized criminal networks; many are individuals working together who may or may not have a personal sexual interest in children.

Once posted, the images are difficult to retrieve. The child has no control over his or her images, and these images can remain in cyberspace in perpetuity.

A significant proportion of child abuse images online are of young children, with an identifiable downward trend in age. According to the IWF 2010 Annual Report, 73 per cent of the child victims identified in online child sex abuse images appear to be less than 10 years old.

Other analyses of online images confirm the preponderance of prepubescent children. There is also evidence that the images are becoming more graphic and more violent. The IWF, for example, found that sexual activity, including rape and torture, between adults and children was depicted in more than 65 per cent of still images and videos found online.

Girls and Caucasian children also figure disproportionately. Studies from Australia, New Zealand, South Africa and the United Kingdom have consistently found that the child sexual abuse images on the Internet are of mostly Caucasian, westernized, female children, 8 to 12 years old.

In much of the research, the main context for the abuse appears to be domestic, and the relationships between those producing the images and the children are familial or of social proximity. (Source of the above – UNICEF)

- 417% increase in reports of child sexual abuse images and video since 2014
- 941 web pages actioned in a single record breaking day

68,092 confirmed as child sexual abuse URLs: 118% increase on 2014

- 2016 report from 57,335 URL’s: 45% were 11 to 15 yr olds; 53% were under 10 yr olds; 2% were under 2 yr olds; 47% were Cat A and B;
- 121 internet industry Members working with us
- Only 0.2% of the world’s known child sexual abuse imagery is hosted in the UK (Source of the above - 2015 Annual Report, iwf.org.uk)
THE COPINE SCALE OF CHILD ABUSE IMAGES (source the IWF.org.uk 2015)

Category A – images involving penetrative sexual activity with an animal or sadism
Category B - images involving non-penetrative sexual activity
Category C – other indecent images not falling within categories A or B

The Deep web and the Dark web:

If you haven’t heard of the dark web before, then you are probably quite unlikely to stumble upon it. It lies beneath the surface of the everyday websites that are accessible via Google and other search engines, in the deep web. It cannot be accessed by traditional web browsers, only via anonymising software, which I won’t go into in too much detail, as I merely wish to inform, not facilitate its use.

The deep web is gigantic and it is impossible to verify how many web pages that are on it at any one time. The anonymity that it provides has made it a labyrinth of criminal activities, some of which directly affect the lives of children and young people. Therefore, it is important for safeguarding and child protection professionals to have at least a basic knowledge of what it is.

Although often used interchangeably, the above graphic highlights the difference between the dark web/net and the deep web. Generally, the ‘Deep Web’ is a generic term for all unindexed web pages that can’t be found through search engines such as Google or Bing. The Deep Web includes many webpages that are encrypted with passwords or documents in formats which is why they cannot be indexed.

Gaining access to the deep web is not a difficult process. The hard part is knowing where to look and where not to look. Access to the dark web is not difficult from here. Due to the illicit and illegal material contained on it, I would advise against even browsing it out of curiosity.

The deep/dark web also makes ‘trolling’ easier. Although sites such as Reddit, 4Chan, Ask FM and to a lesser-extent Twitter are home to many people who hide their identity to antagonise others, the dark web gives them an extra cloak of protection. Countless cases of trolling, often done for sport, which have led to depression, self-harm and suicide attempts amongst vulnerable children and young people.

Besides trolling, the dark web provides child abusers with a means of distributing indecent images of children globally to fellow abusers and has made it easier to do so.

It’s also important to note that up to a third of these images are now generated by the young people themselves whilst sexting and sharing them online. Child abusers source and
curate these images in the dark web. This shows the normalcy of sexting to young people and how it has become a part of their everyday lives, which is another reason the concept of “e-safety” has become so outdated.

It goes without saying, but due to the nature of the dark web, it is important to restrict children and young people’s access to it. It is always a good rule to try and limit the unsupervised access to the internet that a child has. Children and young people are bound to find this secret section of the internet alluring and may want to investigate. To appease the young person’s interest, you could instead persuade them to join a code club for computer programming to develop their interests in a safer environment.

Any post about the dark web would not be complete without a sensationalised tale of the lurid criminal underbelly it houses. Although it is true that many people use the dark web to purchase drugs and other illegal items, the dark web is also used by people who want to remain anonymous for security and privacy reasons. That includes people who may need to shield their identity and communications from surveillance from the state or other agencies, such as investigative journalists or whistle-blowers. The deep web is used daily for a wide variety of reasons by the military, police and activists, among others.

The Dark Web isn’t for spectators and given the illicit and criminal activity that can lurk on it, merely visiting it can be risky.

(Source of the above – INEQE)

Live Streaming Online:

International paedophile rings are exploiting the growth of internet live streaming services to run on-demand child abuse screenings in a “horrifying” new tactic to avoid detection, the chief executive of the NSPCC has warned.

Peter Wanless called for global child abuse networks to be treated in a par with terrorists, employing similar tactics to those used to intercept online communications between jihadists.

He issued the call in an interview with The Daily Telegraph ahead of a conference on new threats to children.

Mr Wanless said police and groups such as the Internet Watch Foundation had made “impressive” progress in combatting traditional child sexual abuse images by using technology to tag the pictures and take them down.

“This has shown that where there is a concerted focus and effort from all sides you can make a palpable impact on the visibility of those sorts of images,” he said.

“But live streaming is completely different, it doesn’t leave a record that you can tag and pull down in the same way.
“In many respects it is doubly horrifying because not only is it harder to track down in that way but it requires the live abuse of children, some incredibly young.

He said that while some recent cases showed that many of those paying to witness child sex abuse were in the Far East, there are believed to be both perpetrators and victims in the UK.

But because the live footage does not leave a digital trail in the same way, the true scale of the problem is still unclear. *(Source - The Telegraph 17/06/16)*

**Periscope – reported threat Jan 2017**

Paedophiles are using live streaming via app Periscope to groom and bombard young children with indecent requests via their mobile phones by paedophiles looking to exploit the youngsters. Minimum age should be 13 yrs to access this app. Twitter’s live streaming service is being used by children much younger than 13 years old. Children can film themselves and post video links on line. Currently there are 10 million users *(source: mail online Jan 2017)*

**Houseparty – app linked to Musical.ly and Yellow**

Houseparty and Chatterbox allows you to arrange events and upload and view shared photos and videos and communicate interacting with a community

**Yellow – phone app nicknamed Tinder for kids**

With more than 7 million users, this app allows youngsters to make friends simply by swiping right or left. If both people agree to “liking” each other then they have “made a friend” and can communicate with them on other chat apps such as Snapchat and Kik. It is linked to Musical.ly and Houseparty. Fears of online predators targeting children have been raised before because people can make up photos and ages. The app is free to download and only asks for date of birth’s name and a picture the app then matches with people of the same age in a radius of 60 miles of where the phone is plotting. Children as young as 10 are using this app and parents and children do not understand the risk. Several Primary schools have been alerted by Police *(source - The Sun online 26 January 2017)*

**Facebook:**

- Worldwide, there are over 1.59 billion monthly active Facebook users, which is a 14 percent increase year over year
- 4.5 billion likes generated daily as of May 2013 which is a 67 percent increase from August 2012
- 1.04 billion people log onto Facebook daily (DAU) for December 2015, which represents a 17% increase year over year
- In Europe, over 307 million people are on Facebook
- Five new profiles are created every second
- There are 83 million fake profiles
- Photo uploads total 300 million per day
- Every 60 seconds on Facebook: 510 comments are posted, 293,000 statuses are updated, and 136,000 photos are uploaded
- 4.75 billion pieces of content shared daily as of May 2013, which is a 94 percent, increase from August 2012
- At 1.49 billion, Facebook has more monthly active users than WhatsApp (500 million), Twitter (284 million) and Instagram (200 million)—combined (Source of the above - zephoria.com)
- In 2016 32 million people in UK have a Facebook page (Source - Statista.com)
- Facebook owns the images even if you close down the site
- IMPORTANT - Facebook can easily be hacked, a UK-based security researcher going by the name of "fin1te" has earned himself $20,000 after uncovering a way to hack into any account on Facebook, just by sending a mobile phone text message (Source – Graham Cluely)

Facebook NEW app – Lifestage – for school teens.

- Members of Lifestage, currently only available on Apple devices in the US, upload pictures and videos based around feelings, likes and dislikes. These are then turned into video profiles.
- All posts are public and there are no options to restrict viewing. The idea is to connect members of the same school, its creator said.
- One expert told the BBC the lack of privacy settings was a concern.
- School members can view each other’s profiles once the individual school has registered 20 members or more.
- Users aged more than 21 are only able to view their own profiles, reports the Tech Crunch website.
- The app warns that it cannot guarantee whether all its users are genuine.

"We can’t confirm that people who claim to go to a certain school actually go to that school. All videos you upload to your profile are fully public content”.

- Lifestage has no messaging functionality but users can display contact details from other sites such as Snapchat and Instagram.

You Tube – 1 billion people now use You Tube (Source – DMR Stats Gadgets) and the site is now very popular with children of all ages.

Whatsapp – This is now secure as it is encrypted so all communication is safe and secure provided the age range law of 16 still applies.

New Sites, Games and Other Activities Considered to be Dangerous:

Checking In:
- When checking in using smart phones, Facebook etc. – abusers can access this info and the Rape Crisis group say that many of their victims were targeted by using it.
- A potential threat comes when children reveal their whereabouts. Predators are nothing if not Internet savvy these days, and if your kid is checking in at a public
location like school or the movie theater — or worse still, at home —they are potentially putting themselves in danger *(Source – blog.kaspersky.com)*

**Baby Monitors** – ensure you have some safety in place as abusers can also remotely access the monitors by nothing more complex than an Xbox 1 from anywhere in the world *(Source - Jonathan Taylor MSc, Social Media & Online Safety Consultant)*

**Webcam** – abusers can remotely access and switch on and off webcams and this will be unknown to the person whose web cam it is. Encourage children to keep the webcam lens covered with a cloth of even blue tack. Young people are increasingly using web cams to experiment sexually. A webcam can be remotely activated by using an X box 1 from anywhere in the world by hacking the IP server.

Ensure your webcam lens is only on view when necessary, if you are using SKYPE or such like *(Source - Jonathan Taylor MSc, Social Media & Online Safety Consultant)*

Regarding Webcams and Cot Cam usernames can be easily hacked - use Safari Browser, they will send a random selection of letter and numbers – not perfect but a lot safer than something you may have chosen.

**Hello Ello! - September 2014:**
- A Q Users flock to new, anonymous social network after Facebook stops its members using fake names
- Created in California for people who are feeling ‘fed up with other social networks’. Requests to join increased from 4,000 to 30,000 in just one week
- Many are believed to be users who had threatened to boycott Facebook for refusing to let them use fake names on the site. Who wants to use fake names, someone with something to hide? *(Source - Mail Online)*

**ASK FM:**
- A Q&A platform where the user sets up a profile and people make statements about them anonymously. Only 1 in 20 of which are good. There is massive pressure on kids to be on ASK FM or they are not ‘cool’.
- Teens are being bullied and a spate of suicides among the young people who used it. The fast-growing social network came under fire after the suicide of British teenager Hannah Smith, whose father attributed her death in part to bullying she endured from anonymous users *(Source – The Verge.com)*

**Whisper:**
- This app allows you to post secrets anonymously and also allows you to chat with other users in your geographic area.
- Many children are drawn to communicating with strangers, feeling that their secrets are safer with them than with their friends. This app is a perfect tool for ill-intentioned strangers looking to connect with young people because it allows you to exchange messages with people nearest to you *(Source – Crosswalk.com)*.
- On 9th Jul 2015 a 12 year old girl was raped by an 18 year old boy in Sussex as a result of having used Whisper *(Source - BBC News)*
• Please don’t confuse the secure version of ‘Open Whisper Systems’ which is a site supported by the government for schools

**Tinder:**
• Users post pictures and scroll through the images of other users. When they think someone is attractive they can “flag” the image. If that person has also “flagged” them in return, the app allows you to contact them
• This app is dangerous and so are similar apps such as Down, Skout, Pure, and Blendr, are primarily used for hooking up. *(Source – Crosswalk.com)*

**Snap Chat:**
• Allow you to capture an image or video and make it available to a recipient for a specific time. After that time limit is up, the picture/video automatically disappears forever...or so Snapchat claims (Similar apps: Poke, Wire, and Wickr)
• Kids can receive (or send) sexually inappropriate photos. This app also makes kids feel like they can “sext” or send inappropriate pictures without consequences because the image will self-destruct automatically. The truth is that nothing sent over the Internet disappears. There are always ways to retrieve and capture those images. *(Source – Crosswalk.com)*

**Snap Maps:**
This location based map allows users to see where in the country their Snapchat contacts are, as well as seeing location based photos and videos. The Snap Map shows a user’s Bitmoji, their cartoon avatar within Snapchat, pinpointed on a world map. Users can then zoom into the map to see the exact location of their friends.

• How to access Snap Maps

To access the Snap Map in the latest update of the Snapchat app, users need to go to their camera screen within Snapchat and zoom out using two fingers. This will then launch the Snap Maps screen and will allow a user to see their friend’s locations.

• Choose who can see your location

It is important to be careful about who you share your location with, as it can allow people to build up a picture of where you live, go to school and spend your time.

Given how specific this new feature is on Snapchat - giving your location to a precise pinpoint on a map - we would encourage users not to share their location, especially with people they don’t know in person.

There are three settings for sharing your location on the map, these are; Ghost mode, My Friends, and Select Friends. But what do these settings mean?
Ghost Mode
Ghost Mode means that you are the only person who can see your location on the map. Within Ghost Mode you can still see the locations of your friends but they will be unable to see you. This setting will ensure that you have complete control over who knows your location.

My Friends
My Friends means that all of your contacts on Snapchat can see your location. If turning on this setting then it would be important for users to review their Snapchat contacts and also make sure that they never add someone they don’t know in person onto Snapchat.

Select Friends
This setting allows users to look through their friend list and then decide which of their friends they want to be able to view their location. This setting gives users the opportunity to control who can view their location.

Changing settings

When first opening the Snap Map users get to make a decision of who they want to be able to view their location. Once these settings are in place they can always be changed in Snapchat’s settings. This can be done in two ways:

In the Snapchat settings
In the Snapchat screen click on the Settings (cog) icon> click on ‘see my location’ > Choose the setting which suits you

On the Snap Map
Click on the setting button in the top right of the map > choose the setting which suits you

Our top tips

Sharing location can be a risky thing to do. Our tips for location sharing are:

• Only share your location with people you know in person. Never share your location with strangers.
• Don’t add contacts to Snapchat if you don’t know them in person.
• Regularly review your settings and take an active decision about whether you want people to know your location. Remember you can switch this off at any time.
• Think about where you’re sharing your location. Location services such as Snap Maps can lead people to your house. Think about what times you’re on the app and whether these are locations you want to share – if not, then turn this off within your settings.
**Vine:**
- Allows users to watch and post six second videos
- While many of the videos are harmless, porn videos do pop up into the feed, exposing your children to sexually explicit material. You can also easily search for/access porn videos on this app. Predators utilize this app to search for teens and find their location. Then they try to connect with them via other messaging apps. *(Source – Crosswalk.com)*

**Fling:**
- Child safety campaigners have branded a new app which allows users to send pictures and videos to random strangers ‘a hotbed for paedophiles’.
- The app can be easily downloaded to phones and tablets – was released in 2014 and is unique because it connects users with randomly chosen people from all over the world.
- When a user ‘flings’ a message, which can include photos, videos or text, it is sent to 50 strangers in different countries around the globe. Worryingly, there is no way to select what age group can receive or reply to your messages – meaning children and adults are mingling with each other. *(Source – Evoke.ie)*

**OoVoo:**
- The world’s largest independent messaging and video chat app. Having been reviewed, the app has been deemed as unsafe for children to use. Users can video call with up to 12 people at a time whilst recording or taking photos, which can then be shared on social network sites. It has a minimum age of 13 years, but only a date of birth is required to bypass this – younger children can easily access it.
- The security is complicated to understand – there are differences between blocking users and deleting them, and new accounts are automatically set to ‘open’, where anyone can see your account. The privacy settings are very minimal, with no guide for parents on their website, but there is an option to view the chat history. *(source – getsafeonline.org)*
- British parents have claimed that paedophiles are using the app to target children – Greater Manchester Police confirmed they are investigating three incidents of sexual activity with a child by an adult using the app. A 10 year old girl was hysterical after a man repeatedly contacted her using OoVoo. The girl witnessed the man performing a sex act and was asked to expose herself and she received missed calls and messages from the man for weeks. *(Source – Mirror.co.uk)*

**Kik:**
- A free app-based alternative texting service that allows texts/pictures to be sent without being logged in the phone history. (Similar apps: Viber, WhatsApp, TextNow)
- Makes it easier for your child to talk to strangers without your knowledge since it bypasses the wireless providers’ short message services (SMS). Children also think they can “sext” without parents finding out. In addition, strangers can send your
**Foursquare** – a location based social networking site that is based on a game like premise, players use smartphones to ‘check in’ to a location, recording their position on a map. See the dangers of using this above (The ‘Checking In’ function).

**Yik Yak:**
- On the surface it seems harmless enough, just another messaging app. The problem with this particular app is that it is an "anonymous" messaging app that allows its users to send text and photos to others without using their name.
- Another feature of this app is that it is location enabled. You can choose to view and contribute to the feed of other users in a 5, 10 or 15 mile radius. This feature can potentially leave the door open for predators to make contact with minors in their local area.
- The "anonymous" nature of this app tends to lull teens into thinking that what they say and share won't be connected to them, which makes them more likely to behave inappropriately.
- Kids have used this app to spread rumors and harass their peers, thinking that they are anonymous. Of course, this isn't entirely the case, and authorities do have the ability to track users. Other worrisome issues include the prevalence of graphic nudity and sexual content. The app encourages users to share just about anything, and because they think it's private, they often do.
- When signing up for the app, users are asked to confirm that they are over 17, however there is no way to verify this, so it isn't any kind of a safeguard. *(Source - UKnowkids.com)*

**Flinch:**
- The idea behind this app echoes an innocent childhood game: Stare at the other person across from you, keep a straight face, and the first person to smile or laugh, loses the match.
- Sounds like oodles of fun, right? Not if the other player live-streaming to your phone is a stranger who could be any age, from any country, and say or do anything in the course of this “game.”
- It’s the bored, mean, seedy people using the apps that take all the fun out of things for everyone else.
- The app, which is now being downloaded and applauded by curious teens, is definitely gaining traction as more of a hook-up app.
- The app might be okay if a user could do a real-time stare down with only an approved friend list. However, Flinch has the option to either: Play a Friend OR Make a Friend it’s the latter that takes this fun game into the danger zone and opens the doors to instantaneous connection to strangers . . . around the globe.
- Random users can track your user name and your location if geo-location is on. That means a user—from anywhere in the world—can locate your child’s school, home, or workplace. Users can easily take screen shots of other users and then essentially use the photos however they wish.
- Many of the randomized “make a friend” users encountered while testing the app...
were men ages 20-40 who appeared to speak very little English. Most were flirtatious. (Go figure—no one wanted to play the staring game).

- Flinch could be—and by all appearances already is—an easy platform for cyber bullies, predators, or criminals to gain access to targets. *(Source – blogs.mcafee.com)*

**Facebook chain link** - you are contacted and asked "are you proud of your child? If so send 3 pictures and then ask 10 friends to do the same", the receiver now has 30 pictures of children. It is a "chain" link post and can be infiltrated and pictures used for abuse images.

**Musical.ly**

- Parents are warning 'paedophiles' are using a hugely popular mobile phone app to groom children'. The free-to-purchase musical.ly app - which has 60m users has been No.1 on the iTunes store worldwide - allows people to create and share 15 second clips and communicate with followers
- The app is used by one in two teenagers in the US and users popularly create lip-sync music videos of themselves singing and dancing - known as "musicals". However, British parents are concerned children have been asked to send naked pictures of themselves to anonymous users within the app
- Mirror.co.uk has discovered two police forces in the UK - in the West Midlands and Merseyside - have launched separate investigations into messages on the app
- The app is clearly rated age 12+ in the iTunes App Store and users can change their settings to private and approve 'followers'. Parents who have spotted the messages on their children's phone have been likewise warning others that they need to make sure that their privacy settings are switched on - and they know people who are 'following' them in real life. They are particularly warning they have spotted deeply concerning messages either sent directly or in the comments section of videos their children have posted. *(Source - Mirror.co.uk)*
- Other concerns have been raised on online blogs by parents about the sexual and swearing content of popular music videos on the app, children are innocently lip-syncing the content

**Lively:**

- July 2016 - Zoosk, the online dating company with 38 million members, a new application aimed at a younger demographic.
- stitched together photo and video collages that tell the stories of its users’ lives., but also other dating apps on the market today, is the way it uses media to enhance users’ profiles.
- The app automatically compresses the photos and videos users upload, then turns them into moving “story” collages, which feature transitions and movement.
- These stories are meant to better show off someone’s personality, lifestyle and interests, without requiring that potential dates swipe through a dozen some photos to get a sense of the person in question. Their animated look-and-feel give the app its name.

**Poof:**

- Hides other apps on your phone. You select which apps you would like to hide and their icons will no longer show up on your smartphone screen
- If children have apps that they want to keep hidden from their parents, all they have
to do is download this app and “poof,” their screen is clear of any questionable apps. So, if you see the poof app on their phone, you may want to ask them what they are hiding. *(Source – Crosswalk.com)*

**Rate My Teacher** – pupils go to this site and do as the name suggests thinking they cause no harm, this can be used very maliciously.

**Retweeting on Twitter:**
- The re-posting of someone else’s tweet, this can be used with any tweets and makes the user’s involvement complicit and active
- It can be used as a way to share useful/interesting/relevant tweets by likeminded services or people, however if a derogatory tweet is posted by one individual, this could be spread to a wider audience by re-tweets
- There are clear guidelines on how to switch off a retweet, disassociating any connection to the users page.

**Layar** - is an app detecting Instagram posts in near-real time in the local area. Once an Instagram picture is selected it will supply information on user and by using the geo-location data of the image a map is provided to the location of where the image was taken. This can be used by child abusers and stalkers.

**Chat Ave** – a free chat room, easy to access with no registration required. The user can click on a photo and speak to random unknown individual who could be from anywhere in world. On the site there are different chat rooms labelled as at ‘Dating’ ‘Teens’ ‘Kids’ ‘Girls’ ‘Boys’ ‘Singles’ ‘Gays’ ‘Lesbians’ etc. The site states 18+ but the chat rooms clearly indicate children are using the site. Users are renowned for asking each other to remove clothes over the webcam and it has become a dangerous portal for child abusers.

**Kiss Chat.co.uk** – a sister site to Chat Ave. The site also states it’s 18+ but everyday girls as young as 11 are being exploited on websites such as www.Kisschat.co.uk. This site and others like it is a hub for older men targeting younger girls for sexual relations online or in person. *(Source - Secure.avaaz.org)*

**GIGATRIBE** – is a peer-to-peer file sharing network and child abusers use this site as a platform to share indecent images of children.

**Chat Roulette** – a similar site to Chat Ave and Fox News has labelled it as a ‘Predator’s Paradise’. Though users of the site must confirm that they are at least 16 years old and that they agree not to broadcast obscene, offending or pornographic material, some legal experts, including one who saw the dangers firsthand, say those barriers can be easily bypassed and can connect children with sexual predators and child molesters. *(Source - Fox News)*

**Omegle**:
- A chat room where the user can talk to strangers via webcam within 35 seconds – self generated indecent images. It even says on the website “Predators have been known to use Omegle so be careful”. Although it suggests anyone under the age of 18 needs parental consent to use the site, there is no verification required and anyone can use it.
Not only are users chatting with strangers, they could be chatting with a fake stranger. “Chat sites like Chatroulette and Omegle have done their best to produce systems that warns users when the people they are chatting to are potentially using fake webcam software, however developers still manage to slip under their radars with frequent updates.” So a fifty-year-old man could set up a fake webcam and use images from a 15-year-old boy that looks like a teen celebrity to convince your child to send inappropriate pictures or get information about your child’s location. (Source – Crosswalk.com)

Instagram:
- You take pictures and videos, choose a filter to change the look and feel and then post it to Instagram
- You can post a malicious or embarrassing photo of a target for all of your followers to see.
- You can caption a gross or disgusting or otherwise insulting or demeaning photo with a target’s username and perhaps a negative sentiment
- You can post cruel comments under a photo that someone posts.
- You can tag a user through the new “Add People” feature on the Share screen – where the tag is added to the image itself. If your Instagram profile is public, anyone can see it – and it could go viral. If your profile is private, and the target is not following you, they will not be notified or be able to see the photo, tag(s), caption, comments. Which could be completely awful, where they are humiliated or harassed until a sympathetic friend finally clues them in.
- You can add hateful hashtags under a photo that you post (in the caption or comments) or that someone else posts
- You can create a fake account to impersonate someone else, and be cruel through pictures, captions, comments, and hashtags.
(Source – Cyberbulling.org)

How to block on unwanted contact on INSTAGRAM – Tap the 3 dots ... on the icon of the person contacting; tap BLOCK; then tap BLOCK again to ensure contact is blocked (source Ineqe group)

HABBO:
A virtual Hotel where you go to chat, play games, make friends, design rooms – 2515 over 13 in UK asked- 57% bullied; 47% threatened, 40% unwanted sexual content ; 20% said they HAD bullied

Bullying through gaming
Called “griefing”. This is when someone damages a person’s buildings, sets harmful traps, or steals all of their items on purpose, just to be mean.

Online Games appealing to Children – such as ROBLOX ; Club Penguin and Moshi Monsters. Abusers masking their ID regularly use these. Where children go – so do abusers, so ensure you monitor your child’s use closely.

Online Gaming - i.e. World of War Craft – playing games with unknown users over the Internet can be dangerous. Abusers frequently mentor the victim suggesting they are able
to get past certain obstacles to help progress the game. Whilst so doing they engage in chat for example – “whilst I am helping you it would be good to know what you look like” or “I can’t do this without your password or at least it will make it easier and faster to do” Not long and there will be a suggestion to meet up. The potential victim is so engrossed in the game they are caught off guard, unaware and readily give over information without thinking. Using gaming headsets encourages abusive, racist, sexualised language, which is only heard by the gamer.

**Minecraft**

**NSPCC - Minecraft: a parent’s guide**  
**Tips and advice for keeping children safe on Minecraft**  
**17 March 2017**

Griefers: The villains. Griefers are human players that intentionally set out to destroy or steal things that other players have built or collected. Griefers can act individually or as a team, entering public multi-player servers with the aim of wreaking as much havoc as possible.

Creeper: Creeper are characters that exist within the game but aren’t controlled by other players. No less annoying than the ‘Griefer’, their only objective is to cause as much destruction as possible. They do this by exploding next to players and damaging anything nearby.

Nether: The dark underworld of the game. Players can build and enter a portal to the Nether. There are some darker elements and it isn’t suitable for young players, as it’s filled with more dangerous characters and hazards.

Whitelist: Like an invite list to your child’s birthday party, a Whitelist lets moderators create a community that only includes people who have been verified to join. It won’t remove the risk, but can reduce the chance of bumping into someone who may spoil the fun.

**Minecraft: the greatest risks and staying safe**

- bullying
- talking to strangers
- hacking
- downloading viruses.

They may also come across inappropriate content like violent or sexual language and images.

To help keep children safe on Minecraft, make sure:

- you know where they’re playing
- they’re using appropriate safety settings
- you talk to them about what to do if they see anything upsetting.
Grand Theft Auto – this site has images of rape and indecent images AND ENCOURAGES SEXISM AND CRIMINAL VIOLENCE SUCH AS RAPE AND BRUTALITY children as young as 4 but mostly from 7 are using this site.

Neo Pets – users must be 8+, it’s a virtual pet game website. It’s an easy place for hackers to access the users pc. Preying on the child’s vulnerability, the hacker will offer them free ‘neo pet’ rewards and then hack the pc. There are websites such as appgamecheats.com, teaching the reader easy ways to hack sites such as neopets.

**Indicators of Risk on the Internet:**
(Source Eyes Open Creative)

- Spending increasing amount of time on Social network sites
- Exchanging inappropriate images in exchange for gaming knowledge-phone- gaming credits
- Arranging to meet people they have met on-line
- Sharing of inappropriate images amongst friends
- Accessing dating agencies via mobile phones *i.e. 02 Flirt Line
- Unwilling to share/show on line contacts
- Receiving gifts through the post from someone the young person does not know
- Concern that a young person is selling images via the internet for money
- New contacts with people out of city
- Concerned a young person’s on-line friendship has developed in to an off-line relationship
- Concern someone is having an on-line relationship
- Concern a young person is selling sexual images via the Internet
- Spending increasing amounts of time with on-line friends and less time with school/neighbourhood friends
- Concern inappropriate images of a young person are being circulated via the Internet
- Concern a young person is being coerced into providing images on a webcam
- Girls with low self esteem are often attracted to inappropriate men

**Text or Internet Codes:** These are used to send messages out quickly, hoping that most of them are not understood by supervising adults:

**BUT do you know a cat’s face image and a knife and fork image means – open invite for sex**

- LMIRL- let’s meet in real life
- IWSN – I want sex now
- 8 - oral sex
- IMEZRU - I am easy, are you?
- TDTM - talk dirty to me
- CU46 - see you for sex
- MPFB- my personal f**k buddy
- SORG- straight or gay
- WYFM - would you f**k me?
- NIFOC - nude in front of computer
- KOTL – kiss on the lips
• 182 – I hate you
• WTPP - want to trade pictures
• MIA – talking about Bulimia
• KMS – kill myself
• 420 - marijuana
• XTC - ecstasy
• MOOS - member of the opposite sex
• AITR - Adult in the room
• MOS - mom over shoulder
• POS - parent over shoulder
• PIR - parent in room
• CD9, CODE9 - parents are nearby
• KPC - keeping parents clueless
• P911 - parent alert
• PAL - parents are listening
• PAW - parents are watching
• ASLP - Age, sex, location, picture
• A3 - Anytime, any place, anywhere
• COBRAS - Come on by right after school
• 9 - Parent watching
• 99 - Parent no longer watching
• NP - nosy parents or no problem
• 121 - One to one
• 143 - I love you
• 53X - Sex
• LOL - Laugh out loud

Advice to Parents and Carers:
Mobile phones – switch of your locations service and frequent locations – the information feeds into the internet which means you can be tracked. SPYWARE can be hacked and you can be tracked and stalked.

• Ask your child – What is on your profile?
  What should not be on a child’s profile: Name, Favourite place, Email address, Mobile phone number, Date of birth, Hobbies, Looking for….., Religion, Politics, Address, Mood, Photo of me, Favourite quotes, Favourite TV programme, Favourite music, Photo of my friends, What am I scared of, Favourite film, Relationship status, School, College
• The above list can be dangerous as it can help an abuser to identify a child’s location through their interests etc. (Source - University of Bedfordshire Cyber Research department for Stalking and Abuse)
• Ensure your child is prepared if you state you are homosexual – it is an immediate target for cyber bullying
• UNDERSTAND THE DEVICE IN YOUR CHILD’S POCKET AND WHAT IT CAN DO
• If a child has been a victim of any form of online abuse - remember to save the evidence and confiscate the child’s device so there is a trail which can be proved by Police
• Play the on line games with your child so you understand and can overview and have a sense of what be happening
• ask your child why he/she thinks you are anxious about the Internet – see what they say, try and ascertain if they understand about the hidden dangers
• DO NOT ALLOW INTERNET ABUSE TO DISTRACT YOU FROM THE VERY REAL HARM AND STILL MORE USUAL ABUSE OF INTRA FAMILY AND FRIENDS/ASSOCIATES AS ABUSERS

We need to educate children not to give in to peer pressure to:

• get into a car with someone you don’t know
• kiss someone you don’t know
• get a taxi alone
• have unprotected sex
• go alone to a house you don’t know
• accept a drink from someone you don’t know
• accepting gifts from someone you have just met
• meeting someone you don’t know
• giving out your mobile number to someone you don’t know

Guidelines & Restrictions to Protect your Child:
(Source – Be Safe Online, Jonathan Taylor MSc, Social Media & Online Safety Consultant)
‘Wherever you child goes online so should you.........’

These guidelines can be used by parents wanting to protect their child from the many online dangers that can exist. Children vary from being the most vulnerable child to the most resilient. Understanding where your child sits on the Spectrum of Vulnerability is the first step to knowing the level of protection required.

These are guidelines and designed for parents to use when required:
• Set limits on when they can use the computer and for how long.
• Agree what types of sites are permissible and which are not.
• Encourage them to come to you if anything online makes them feel uncomfortable or threatened.
• Make it very clear that they must not give out personal information without your permission. In particular, addresses, phone numbers, school details, passwords or pictures.
• Warn them to be careful about giving away their email address in chat rooms or when registering for sites.
• Forbid them to meet anyone in person that they encounter online without your consent and without a responsible adult present.
• Agree what types of sites are permissible and which are not; for example you may make a policy of not allowing them to use un-moderated chat rooms or to use file sharing programs.
• Restrict their ability to download software, music or other files without your permission. (Big difference between iTunes & File Sharing Systems)
• Agree whether (or not) they are allowed to spend money online. Although you might not give them your credit card, if you have already stored your details at an online store it may be easy for children to spend your money if you don’t take steps to limit their access or agree ground rules.

• Explain what viruses and spyware are, what you are doing to prevent them and ask them to come to you if they get an alert while online.

• Research age-appropriate Internet sites that you can suggest to your children.

• Adult to set up email and password, to allow for access, updating or changing when need arises. (For all sites that require email log in)

• Remember computer can be set up to allow user to automatically log in.

• Email username not to include identifiable features such as (amy_14_leeds...)

• Adult to set up MSN account using avatar not real image, and only allow max of 15 contacts, (see last guideline) all should be known or had identity verified, (e.g. school, club friend or family)

• Messenger service (MSN or Yahoo) to be set up so as to save chat history, and should be periodically checked (for any offline messages).

• SNS profiles to be created by adult so as to be in control of password, to allow for access, updating or changing when need arises. Computer can be set up to allow user to automatically log in. Allow membership to just ONE site.

• SNS profile not to include image of user on home page (Un 16). Profile to be set to private, however remember some SNS do have facility to show who is online. Password to kept by parent / guardian to allow for access, updating or changing when need arises. Remember computers can be set up to allow user to automatically log in. No personal details on site...Email / mobile /address / school / clubs / age...etc.

• Parent / Guardian to become members of the same site, either with or without correct details, photograph to be included.

• Add son / daughter as friend / contact, and they must accept you.

• Parent / Guardian to add their profile and photograph to home page of son / daughter, for all child’s contacts to see, perhaps with heading ‘My mum / dad who sometimes comes on as me to check...etc’.

• Every 2 -3 weeks log on as the younger user and make it known that you are not them and are there to check.

• Chat facilities, Web Cam Chats, File Sharing Systems should NOT be used, even if they state they are for children only. The users are only electronically verified and so anyone can join. Chat facilities do not require profiles and allow for complete anonymity.

• Consider limiting the amount of friends son/daughter allowed to invite / accept dependent on age; e.g. (11-13 yrs = 30 contacts) (14 yrs = 40 contacts) (15 yrs = 50 contacts) (16 yrs = Unlimited but monitored)

WWW – means exactly what it says – World Wide Web:

• 8 years ago there was no social media and we still haven’t realised we lose control the minute the Internet is used to post any information/images about ourselves, this is there for the world to see forever!

• If people were more Internet savvy many of these on line crimes would not happen
**Guidance and safe Resources:**

- Educators in On-line protection - [www.mydangerousloverboy.com](http://www.mydangerousloverboy.com)
- H2b safer for professionals from INEQE free updates [http://us7.campaign-archive1.com/?u=8c3ff982b241ebd9256f18e39&id=fd42723fb5&e=ce45d4db4f](http://us7.campaign-archive1.com/?u=8c3ff982b241ebd9256f18e39&id=fd42723fb5&e=ce45d4db4f)
- [www.ineqe.com/apps](http://www.ineqe.com/apps) and [www.ineqe.com/ssnap](http://www.ineqe.com/ssnap) and [www.ineqe.com/digital-footprint](http://www.ineqe.com/digital-footprint) INEQE provide a vast range of excellent resources and on line training for schools
- [www.childnet.com](http://www.childnet.com)
- [Netaware – NSPCC](http://www.netaware.org.uk) for 8 to 12 year olds
- [The Northern Ireland Safeguarding board](http://www.ineqe.com/) has developed excellent apps for support says Jim Gamble CEO of INEQE
- [Action for Children](http://www.actionforchildren.org.uk) supports and speaks out for vulnerable children and young people in the UK. Action for Children NetSmart has useful tips about keeping safe online.
- [Information to support parents and carers to understand and respond to the risks children face as they grow – www.thinkuknow.co.uk/parents](http://www.thinkuknow.co.uk/parents)
- [CEOP](http://www.thinkuknow.co.uk) - new video – Romeo and Juliet – free to download helpful to parents [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
- [INEQE GROUP](http://www.ineqe.com/) - CEO is Jim Gamble, international expert, the website is exclusively targeted at staying safe on the Internet and various apps and how to block and report
- [www.thinkuknow.co.uk – “the world changes – children don’t” – talk to your child about sex; relationships and the Internet](http://www.thinkuknow.co.uk)
- [CEOP UK – new sept 2016 “sexting guidance in schools and colleges – responding to incidents” produced by the UKCCIS – UK council for Child Internet Safety](http://www.thinkuknow.co.uk)
- [www.screenagersmovie.com – resource](http://www.screenagersmovie.com) SCREENAGERS dives deep into how technology impacts child development and the challenges of parenting in the digital world.
- [LEICESTER POLICE FILM](http://www.thinkuknow.co.uk) - Film warning about online grooming - date 03 January 2017 :

**“ Kayleigh’s Love Story “**

Leicestershire Police has made its film to raise awareness of the dangers of online grooming publicly available. Based on the story of teenager Kayleigh Haywood, the film highlights how quickly and easily children can be groomed online without them or those around them knowing it is happening. Kayleigh’s love story is available to watch online in eight different versions, including a signed version, and audio described version and versions translated into five languages. It has previously been shown to schoolchildren aged 11 and above in Leicester

• **CEOP - Think You Know films** – “Jigsaw” is for parents, “Exposed” is about “Sexting” “Sam’s Real Friends” is for those with learning disabilities and special needs

• You can download *Nude Selfies: What Parents and Carers Need to Know* now! You'll find it under the 'Parents' tab in the Resources section of your online account at [www.thinkuknow.co.uk/teachers/resources](http://www.thinkuknow.co.uk/teachers/resources)

• For advice to teachers, parents and teenagers on how to deal with cyber bullying - [http://cyberbullying.org](http://cyberbullying.org)

• **Teachtoday** provides information and advice for teachers, head teachers, governors and other members of the school workforce about the positive, responsible and safe use of new technologies.

• **Teachernet** has published guidance written by Childnet International for the Department for Children, Schools and Families about cyberbullying and advice on ways in which school staff can be protected.

• **Childnet International** is the children's internet charity committed to helping to make the internet a great and safe place for children.

• **Click Clever Click Safe** is a UK Council for Child Internet Safety campaign aimed at young people and parents.

• **Get Safe Online** is a joint initiative between the Government, the police and private sector sponsors finance to provide user-friendly advice about online safety for consumers and smaller businesses.

• **Insafe** is a European network of Awareness Centres promoting safe, responsible use of the internet and mobile devices to young people.

• **Marie Collins Foundation** is the charity to contact who deal with online victims: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk)
  
  EMAIL – [admin@mariecollinsfoundation.org.uk](mailto:admin@mariecollinsfoundation.org.uk) OR [collmar2014@gmail.com](mailto:collmar2014@gmail.com)
  
  Phone – 01677 460168

• Albert Kennedy Trust: AKT supports young LGBT 16-25 year olds who are made homeless or living in a hostile environment. New on line help and advice service

For further information on training or assistance please contact MARILYN HAWES CEO and FOUNDER of EAUk:
[www.enoughabuseuk.com](http://www.enoughabuseuk.com)

Marilyn.hawes@ea-uk.org - Mobile - 07484 541727