#DITTO

STAY SAFE ● HAVE FUN ● REPEAT

EDITION 21 - NOV 2019

In this edition

www.esafety-adviser.com

Foreword from Alan Mackenzie

Welcome to Edition 21 of #DITTO

Hi there, I'm Alan Mackenzie.

I'm an independent consultant specialising in online safety, specifically within education to children, young people, schools and other organizations, and parents.

I'm a strong believer that technology, for the most part, is neutral; behaviour is the most important aspect.

To understand behaviour, we have to be a part of children's lives in order to understand what they're doing with technology and why.

We have to be curious and guide them to realise the wonderful opportunities that the online world gives to all of us, and be there to support them when they need it.

Contact Alan

01522 25 30 88

www.esafety-adviser.com

alan@esafety-adviser.com

twitter.com/esafetyadviser

facebook.com/esafetyadviser

If you've been reading DITTO for a while, or if I have visited your school to talk to the students, staff, parents or governors, you will know that I always talk about technology in a positive, upbeat way.

Primarily this is because I'm a fan of technology and always have been, but also I don't like to talk about the risks and issues without properly balancing the positive aspects too, particularly when talking to students who will simply switch off if all they hear is "danger, danger" type talks.

Whilst some of the risks and harms that we see are very serious, in the overall scheme of things the balance is firmly weighted towards the positive, meaning that the majority of children will take risks, that's a part of growing up, but won't come to harm.

But sometimes technology advancements come along which stop me in my tracks to re-evaluate my thinking. One of those advancements is deepfakes and (closely related in my opinion) artificial intelligence generated influencers.

I see no benefit with this technology, but I do see the potential for significant harm. I could be wrong, but only time will tell.

Alan

OPINION

Deepfakes

Technology evolves at an extraordinary pace. That's a pretty obvious statement, but does it always evolve in a way that is positive and to the benefit of all? I'm not so sure, and when it comes to deepfakes I can see no positive use whatsoever. Quite the contrary in fact, I see this technology being used for very significant harm; it's already been used in such a way.

It goes without saying that if it wasn't for marketing and advertising we wouldn't see the online world as we currently do, and it certainly wouldn't be free or low cost as it currently is.

As an example, what is Google? You'd be forgiven for thinking that it's a service that provides you results based on a search query. What is YouTube? It's a service that allows you to search for and view videos on gazillions of topics.

Those answers are correct, but first and foremost Google search and YouTube, as well as many other online services such as Facebook and Instagram are advertising platforms which serve us content based on a multitude of algorithmic variables.

So it's no surprise that advertising and marketing are always pushing the boundaries of evolving technology to reach bigger audiences in order to socially engineer us into purchasing something.

The ability to manipulate images has been around for a long time; as a photographer I

use photo manipulation to enhance images all the time, much like historic darkroom techniques but in a digital form, such as removing skin blemishes in a portrait, biscuit crumbs from around the mouth of a dog, or enhancing a sunset in a landscape photo to make it look more dramatic.

More recently we've seen apps that can face swap; these are mostly used for a bit of fun but equally we've seen them being used for inappropriate purposes too, such as bullying and sextortion.

But this is nothing compared to deepfakes; we're at a whole new level of abuse and when this technology becomes more mainstream and quite frankly I'm worried.

Imagine finding a video of yourself starring in an x-rated movie where your face has been superimposed onto someone else and it looks unbelievably realistic, but not only your face, your expressions and your voice too.

Welcome to deepfakes.

This is a whole new level of fakery; through deep learning, computers can generate convincing representations of something that never happened. Traditionally the technology needed large quantities of high quality images but earlier this year Samsung announced that their AI system could produce deepfakes with just one photo. How difficult is it to find a photo of an individual online? And it isn't just the visual aspect, it's audio too, and this adds a further dimension of reality. But it doesn't stop there, the technology to detect deepfakes is a long way off.

According to many online sources such as Wired and The Economist, the term deepfake first appeared on a Reddit forum in 2017. It was the username for a person who was producing fake videos of female celebrities having sex. Whilst the account was eventually removed from Reddit, a lot has happened in two years.

During June and July 2019, a company called Deeptrace carried out a study finding almost 15,000 deepfake videos, of which 96 percent were pornographic. All the videos were of women and many of these had millions of views. This is twice as many as seven months earlier and horrifyingly they also found deepfake forums where users are discussing and requesting deepfakes of women they know, e.g. ex-girlfriends. This is a violation on so many levels.

There's a lot of talk around deepfakes in the media, but this is mainly from a political perspective rather than child protection, specifically in regards to concerns over the forthcoming election. I understand the electoral concerns, but the implications for young people, especially girls, are far-reaching and potentially lifelong lasting.

Sadly we're living in a world where we have to mistrust everything we see and hear online until we can prove otherwise .

You have got to wonder at the morals and ethics of the companies that are forging ahead with developing this technology without a single thought to the potential for negative implications. There's a lot of talk about 'safety by design' at the moment and I would have to agree; companies need to be working to a moral code of conduct and hopefully (election not withstanding) we might start to see some action when (if!) the Online Harms Bill is brought into law.

So how can we start talking about this with children and young people, whether in school or at home?

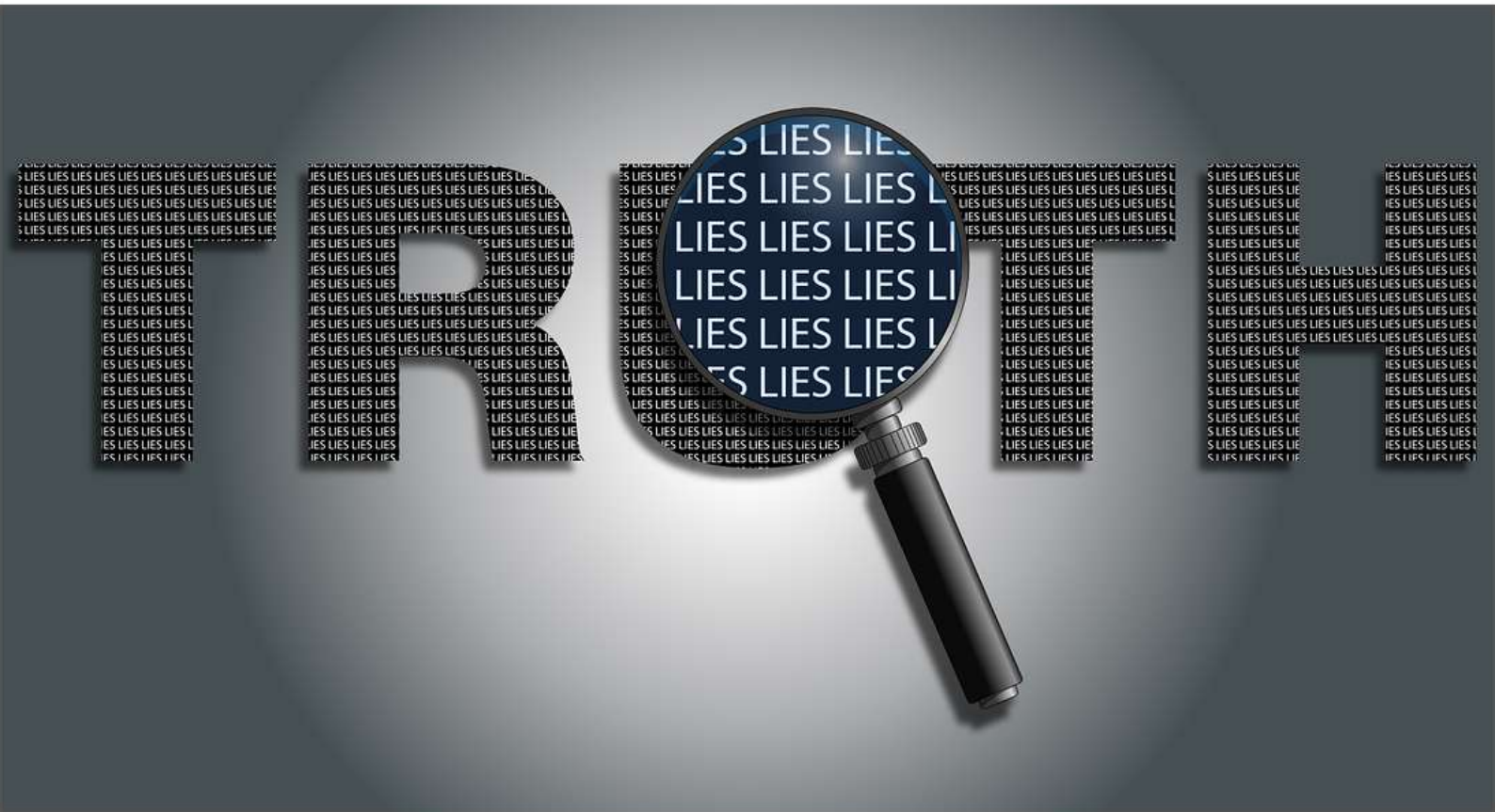
Personally I would be introducing it as a topic for discussion and debate in order that the positives (if any) and the negatives can be openly discussed. Within this you could introduce how easy it is to find photos of people online (digital footprint), the ethics of companies developing and using this technology, the rights of the child; what would 'safety by design' look like in this case?

To see deepfake in action, search on YouTube for the following (these are not explicit):

- Obama deepfake
- Zuckerberg deepfake

And to see a really good explainer video search on YouTube for the TED video, 'Fake videos of real people' by Supasorn Suwajanakorn.

Alan Mackenzie



Online Safety PRO

The only course of its kind; unique and engaging.

Keeping you, your staff, governors and parents up to date.

A 1-day upskilling course for your online safety lead covering a range of topics including:

- Risks and opportunities related to gaming, YouTube and social media.
- Whole school approach to managing online safety.
- Engaging children and parents.
- Best free resources to use in the classroom
- and much, much more.

PLUS:
Unlimited 12 months access to online training for:

- All teaching staff.
- All support staff.
- All governors.
- New joiners during the 12 months.

- **Plus** a regular 10-minute video to keep all your staff right up to date.

The course is delivered by Alan Mackenzie

27th January 2020 - London
23rd April 2020 - London

For more information:

http://www.esafety-adviser.com/onlinesafetypro

SNIPPETS

Call of Duty Modern Warfare was released mid November. It is the latest release in a long line-up of massively popular games and given its popularity it's no surprise I'm already talking to Years 4, 5 and 6 (8-11 year olds) in schools who are playing it.

As you would expect given the age rating of 18 it can be really violent; it includes terror attacks in Piccadilly Circus and child soldiers in the Middle East.

These types of games are often controversial and there will always be different opinions about the content and realism, but the bottom line is that the game is rated 18 for a reason.

Parents - check games settings on devices so that your children can't download these types of games without your permission. If you don't know how to check settings on particular devices, go to the Internet Matters website for guidance.

SafeToNet FOUNDATION

Podcast

CYBER-ABUSE PREVENTION & REHABILITATION
Registered charity No: 1179486

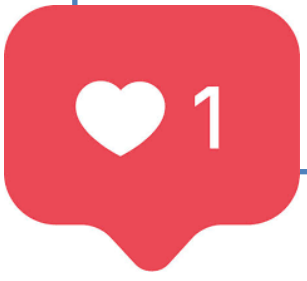
I'm on the road a lot and enjoy listening to podcasts on those long journeys. A not-to-be-missed podcast is from the SafeToNet Foundation which focuses on safeguarding children in the online digital context. Covering topics such as cyber-abuse, bullying, sexting, wellbeing and much more it is a wonderful free resource to keep up to date on many issues.

https://safetonetfoundation.libsyn.com/

Instagram Likes - In a bid to improve the mental health and wellbeing of young people and adults, Instagram is testing hiding the amount of likes a user gets on a post. The thought process is that it will allow users to concentrate on content rather than a competition for likes akin to a validation.

The testing has been ongoing since 2018 but we're just about to see it here in the UK according to recent reports. Unsurprisingly influencers are up in arms about this, worried that they will lose followers and therefore income.

Personally I'm on the fence at the moment. It is only the account followers that have the likes hidden, the person posting the content will still see the amount of likes. Time will tell if this has any positive impact so we'll just have to wait and see.



PROJECT EVOLVE

FOR SCHOOLS

You will hopefully be aware by now of the UK Council for Internet Safety (UKCIS) - Education for a Connected World framework which came out early in 2018 and the guidance from DfE 'Teaching Online Safety in Schools' which makes multiple references to EFACW. The framework isn't just about online safety, it considers much more under 8 strands (and 330 statements) of online life for every year group:

Self image and Identity.

Managing Online Relationships.

Online Reputation.

Online Bullying.

Managing Online Information.

Health, Wellbeing and Lifestyle.

Privacy and Security.

Copyright and Ownership.

You may be wondering, "How do I plan to cover all of that?" Help is here; South West Grid for Learning have been working tirelessly for some time to develop the free resources to assist you and by the time you read this, the first 4 strands should have been released with the final 4 to come in early 2020.

The text on the following pages has been reproduced with the permission of South West Grid for Learning.

What is Project Evolve?

ProjectEVOLVE resources each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" with perspectives; research; activities; outcomes; supporting resources and professional development materials.

This vast library of content is managed by an innovative new engine, designed by the brilliant SWGfL Webteam, that not only makes navigating the content intuitive but allows users to personalise the content they collate.

Just need a research summary on a topic? What about a lesson plan with stimulus questions? How about activities for pupils and students? Professional development materials for your staff at the press of a button or screen tap. It has been designed with customisation and flexibility at its heart.

The vibrant new content has been written by a team of experts here at the UK Safer Internet Centre. It's up to date; relevant and engaging and moves online life education into the third decade of the 21st century.

PROJECT EVOLVE

Why Project Evolve?

We find ourselves in a world where information drives society and for many media businesses, it's a valuable commodity. Navigating this complex landscape is difficult at best. Many of find our way through this tangle of information through trial and error; forging our own unique path and learning as we go. However, as we have seen only too often, some of those errors have the potential to lead to harm.

It's no accident that Media Literacy; Digital Literacy and Citizenship are a key element of the UK Government's Online Harms white paper. Amongst a raft of other regulatory measures, Media Literacy education threads itself through the whole strategy. But what does good digital literacy education look like?

Eight years ago there was no Snapchat; no TikTok; no 5G; no Cambridge Analytica and who would have thought we would be worrying about fake news across the whole media landscape? Ransomware hadn't raised its ugly head and the prospect of deep fakes hadn't emerged.

Gaming had not yet experienced the online ascendancy of GTA V or Call of Duty and 'Blue Whale" was still six years away.

Gradually, Digital Literacy became more difficult to update and less relevant each passing month. Time for a rethink!

Project Evolve Principles

UK Safer Internet Centre had worked with the UKCIS Education group to create the framework "Education for a Connected World" released by UKCIS and UK government in February 2018. This was a radical refocus on what our expectations and the outcomes should be for children and young people when educating and supporting their lives online.

The framework is challenging, relevant and detailed with over 330 statements covering an age range from 3 years old right up to 18. Eight strands cover all aspects of online life:

- **Self Image and Identity:** shaping online identities and how media impacts on gender and stereotypes.
- **Managing Online Relationships**: relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
- **Online Reputation**: strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.
- **Online Bullying**: strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation.
- **Managing Online Information**: offers strategies for effective searching, critical evaluation and ethical publishing.
- **Health, Wellbeing and Lifestyle**: understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.
- **Privacy and Security:** behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.
- **Copyright and Ownership**: protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

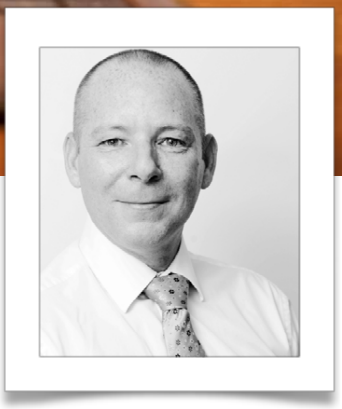
Whilst the framework is clear and builds on prior learning, professionals are left to their own devices in interpreting statements and planning lessons, activities and outcomes. And there's so much of it!

Having been at the heart of the framework since its inception, ProjectEVOLVE has been developed to compliment the UKCIS framework and support all those who work with children and young people to bring those statements to life.

Influencers

Increasingly we're seeing a rise in so-called influencers, usually described as somebody who has established credibility in a specific industry or genre, e.g. make-up, toys, gaming etc. Many of these influencers are genuine, down to earth people who simply want to share good advice and make an honest living. However, for us parents and school professionals the clue is in the name, influencer: a person with the ability to influence potential buyers of a product by promoting or recommending items. Equally it may be to influence a behaviour such as carrying out a challenge. As with anything like this, there are the good, the not so good, and those that wish to exploit children.

Commonly when speaking with children, the most-watched genres of videos tend to be how-to's, gaming, challenges and general fun videos such as 'try not to laugh'. But also, videos about their hobbies such as slime, horse riding, gymnastics and much more. On social media it tends to be their friends and celebrities or influencers.



These influencers are aware of this and will target children with the most popular genres in order to increase engagement such as views, likes, comments and ultimately subscribers. The purpose is simple; more engagement means more ad revenue and potentially revenue from sponsors for things such as product placement, mentions, reviews etc. and whilst the various social media outlets require channels to be clear when something is being advertised, the reality is that many of these influencers don't make it clear.

This is an understandable concern for parents, however in my experience speaking with children, they're pretty clued up when it comes to this form of advertising, often using statements such as, "They're just trying to sell their merch (meaning merchandise)."

There's another side to this also; you may well have seen in the media in the last few weeks references to 'sadfishing'. I'll cover this in more depth in another edition, but simply speaking it's being described as a new phenomena online where people are posting things such as, "my life is terrible," "I'm having such a bad day," "none of my friends like me," and the list goes on.

Suffice to say this isn't new, it's normal behaviour which just happens to be shared online, but there are potential consequences such as offenders capitalising on the vulnerability and using that to gain friendship and trust with a child (grooming).

Sadfishing became prominent a couple of years ago when a very well known celebrity was posting on social media about some of the troubles she was going through, but without going into any detail, and stating that a big announcement was coming. Basically it was clickbait; keep the details out, get the rumours going, increase the engagement.

After a couple of weeks, the announcement was finally made. The celebrity was talking about the difficulties she faced as a teenager with her skin; a problem that almost every teenager goes through and it can be a very difficult time for some. But what wasn't so obvious was that this celeb had gone into partnership with a skin care company and was being paid huge amounts of money! Brilliant marketing, questionable morals.

But as time moves on and technology evolves, so does the way in which that technology is being used, for example AI (artificial intelligence) and CGI (computer generated imagery). You may have read the previous article about deepfakes, where images of individuals (usually female celebrities) are mapped onto the face of an adult (sexual) performer.

These videos are concerningly realistic, it's very difficult to tell that they're fake. But within CGI we're also seeing a rise in fake influencers too. For example, take a look at 'Lil Miquela' on YouTube or Instagram where she

has 1.6 million followers. It isn't difficult to see that Miquela is computer generated. You may be forgiven for thinking the images are of a real person and filters have been a little over-used, but the videos clearly show that it's CGI if you look carefully. What's more, advertising agencies are using the likes of Lil Miquela to 'influence' their products.

You might be asking why use CGI? There will be many reasons, but cartoons have always been used in the past to engage with children and young people, this just seems to be a modern version of that, albeit a much more realistic version, for example Lil Miquela has made music videos, has hung around with real celebrities and was even voted as one of the top 25 most influential people on the Internet in June 2018 by Time magazine.

Along with deepfakes, this is a level of fakery we haven't seen before, and there are more and more AI influencers out there who are even interacting with each other. It's mind boggling. We're only just getting to grips with teaching children about fake news and now we've got this to contend with.

So how do we teach children what is real and what isn't or virtual?".

A lot of it comes down to simple critical thinking, the same logic we apply into any area of our lives; we ask ourselves simple questions, such as:

- What is the purpose of this image/video?
- Is there a point to the video, image, or message? Are they trying to influence you in some way.
- Is it opinion or fact?
- Why are they talking about this product?
- Does it say something like 'paid partnership' or 'in partnership with….' above the video or image, or sometimes in the text?

To see a more in-depth explanation about Lil Miquela, search on YouTube for a video by Colin and Samir called 'Lil Miquela Exposed'. It's quite eye-opening.

Alan Mackenzie

GoBubble

Safer, healthier, kinder social media experience GoBubble has revealed its 2020: Year of Digital Wellbeing initiative, designed to support childrens' online welfare.

The socially responsible brand is calling upon schools, digital allies and friends to declare their support for the digital wellbeing of kids across the world, by signing up to an online pledge.

Supporters will receive learning resources, information and a badge!

To find out more, or commit your support to GoBubble's 2020: Year of Digital Wellbeing programme, visit:

https://gobubble.school/channel/digitalwellbeing

IWF
Internet
Watch
Foundation

I've seen parents use it, I've seen teachers use it, I've seen safeguarding leads use it, but most of all it's the media that is, by far, the worst offender and should know better. I despise the phrase, it makes me cringe every time I hear it being used.

The IWF are campaigning for an end to the use of the phrase 'child pornography'. Pornography is pornography; the use of the word child implies consent and yet, as the IWF correctly state, children cannot be complicit in their own abuse.

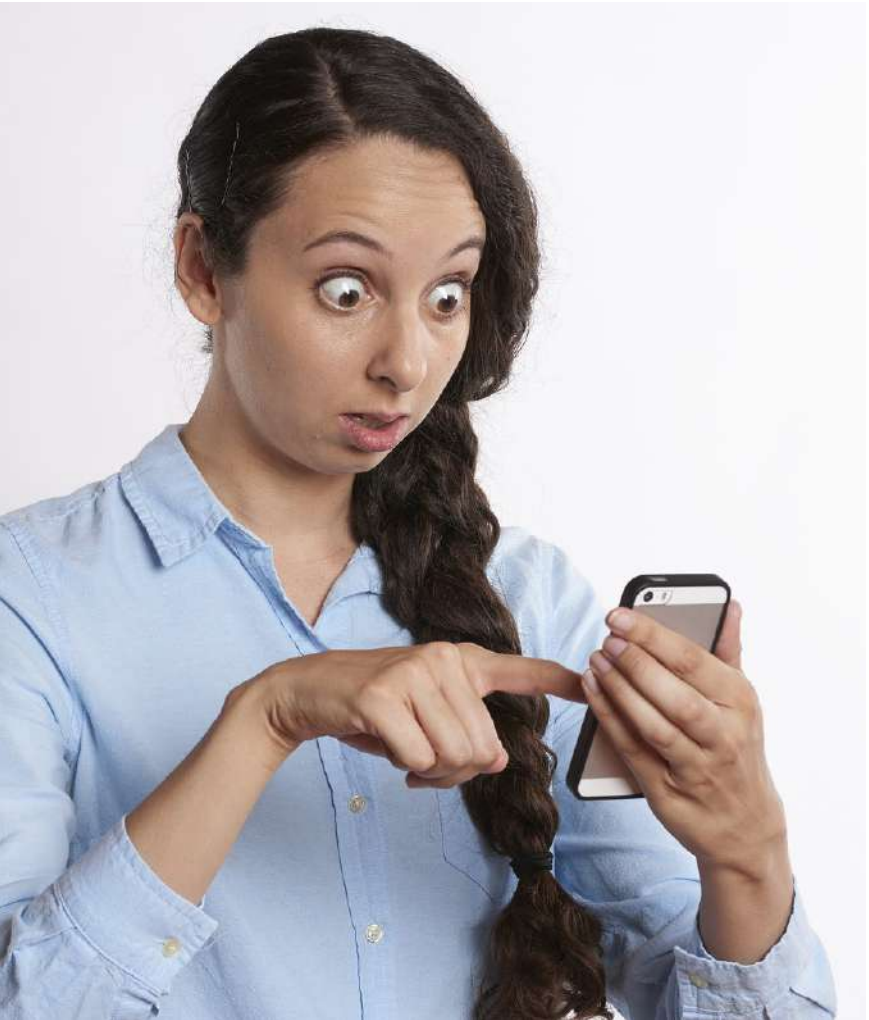
The IWF are asking all of us to take action and spread the word. See the link for more information:

https://www.iwf.org.uk/nosuchthing

DOING IT TOGETHER

Notifications and Immediacy

A couple of weeks ago I was speaking to some children in a class about messaging and notifications, amongst other things, and one child was clearly upset that when she sent a message to her friends (usually to a WhatsApp group), she could see the double tick (denoting the message had been received and read) but there was no immediate replies to her message.



The statement from the child came out of nowhere so it was something that had obviously been playing on her mind for some time, but it did allow us to have a chat and put her concerns to rest, such as people can't always reply immediately.

There definitely seems to be a sense of immediacy and it isn't just with children. I've done it myself, send a message, see the tick that it has been received, sit there with fingers drumming wondering why the person is ignoring me? What have I done? Am I in trouble? I'm sure there must be some psychological theory behind this.

In the same conversation the children were talking about how many messages they receive overnight, sometimes waiting to be answered in the morning, sometimes answered during the small hours. These numbers (of messages) are up in the hundreds, with some children saying it makes them feel anxious, that they feel pressurised to respond immediately. Others say it doesn't bother them at all.

Have a chat with your child. How many messages do they get each day, do they feel pressurised to answer, even during the small hours? Is this having an effect on wellbeing?

RESOURCES FOR PARENTS

I'm quite often asked what the best resources for parents are. Not an easy question to answer as it would depend on what your concerns are, your level of knowledge, or a particular risk that you would like more information on.

Below are 4 of what I believe to be the best, current and up to date resources.

Common Sense Media
To learn more about the games or apps your children are using, Common Sense Media covers thousands, which includes advice and reviews from other parents:

https://www.commonsensemedia.org/

Internet Matters
Tons of age-specific related information created specifically for parents. Includes information to set up devices.

https://www.internetmatters.org/

YouTube
With over 5.5 billion videos, if you need to know something there's a good chance it's here. Use simple searches such as, "What is…" "How do I…"

https://www.youtube.com

School
The school your child goes to is a wealth of information. If you're not sure or don't know where to turn to, they can and will help. Find out what what your child does in school about online safety so that you can replicate the same advice at home.

Contribute to the magazine

I'm always on the lookout for great content to share with schools and parents, but I also know that people have their own individual stories to tell. This information can be hugely beneficial for everybody.

- Are you a parent who has experienced something with your child? What was it and what did you do? Has your child experienced something and would he/she like to share their advice with others?
- Are you a school that has experienced a series of incidents? How did you tackle this? Do you have an innovative way to engage with specific online safety topics in the school?
- Do you have an opinion or a thought-provoking idea?

Drop me an email and let me know your thoughts. Everything can be kept anonymous if you wish.

Alan Mackenzie

alan@esafety-adviser.com

www.esafety-adviser.com

Contact Alan

01522 25 30 88

www.esafety-adviser.com

alan@esafety-adviser.com

twitter.com/esafetyadviser

facebook.com/esafetyadviser