SCHOOLS NEWSLETTER – NUMBER 1 – BLACKBURN SCHOOLS

By Marilyn Hawes Founder and CEO of Enough Abuse UK – marilyn.hawes@ea-uk.org

Hello to you all !

With the constant media attention given to case upon case of child sexual abuse, exploitation; images; I felt it a good idea to create a newsletter to despatch to you all with any updates and things of interest relevant to you as educators, carers; parents in the Blackburn area.

I have become known to several schools in Blackburn for the last year and I always enjoy revisiting and am due to do so from 12 March 2017.

This week I have been greatly involved in challenging the proposals from Chief Constable Simon Bailey to withdraw on sentencing on what he describes as "low risk offenders viewing low category images"

Therefore, I decided information known to Enough Abuse UK should be shared among you .

ALL child abuse images mean a child has been violated and abused. We MUST NOT minimise the severity of this crime due to lack of resources. Often the viewing of images transfers into hands on abuse

In order to PREVENT child abuse, PREVENTION education is ESSENTIAL. This is the work we offer and deliver with great success across the UK.

However today, I thought I would send you extracts of the various danger hot spots from our DIGITAL GENERATION document.

Going forward it may be a good idea for you all to contact me with any topic of interest pertinent to your school or life or experience etc. This way we will engage in a worthwhile project of learning and I can write your questions and my answers in a monthly or fortnightly newsletter.

LET'S KEEP THE CONVERSATION GOING – follow us on TWITTER @enoughabuseuk

NSPCC – 1 in 20 children report being sexually abuse in the UK

1 in 5 children report other forms of serious abuse in the UK

I AM HOPING by engaging with me thought this newsletter, in facing the issues of this heinous crime, children in BLACKBURN will benefit

APPS TO AVOID OR USING GREAT CAUTION – EAUK DIGITAL GENERATION DOCUMENT EXTRACTS

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)*

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:

- newChild 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 worlds 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 child a "friend request." *(Source – Crosswalk.com)*

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 – 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)