Corbets Tey School

Technology and Online Safety Newsletter

Edition Number: 6 **Month: May 2017**

The Department for Education guidance document **Keeping Children Safe in Education (May 2016 updated Sept 2016)** sets out the legal duties with which schools and colleges must comply in order to keep children safe including keeping safe online.

We are aware of the special challenges for our parents regarding online safety. We want to work in partnership with you to identify where additional support and information is needed and how to use this to protect your children and young people. This regular newsletter will ensure that you are aware of the latest developments and information available.

Safeguarding – Hoaxes and Fake News

You may well have seen news and social media posts about **'Blue Whale'**, the posts urge you to share to protect young people from a viral suicide game. https://www.thesun.co.uk/tech/3003805/blue-whale-suicide-game-online-russia-victims/. The 'Blue Whale' story is a hoax, or fake news, something which is permeating almost every news area recently. http://www.netfamilynews.org/blue-whale-game-fake-news-teens-spread-internationally

Alerts are often shared over social media, even when initially shared through more conventional routes, such as letters home to parents. The danger with a social media share of a hoax or fake story is that it will also reach young people. There are significant pressures caused by FOMO – fear of missing out; this affects body image, feelings of belonging and for a young person with poor mental health it may encourage them to consider or copy a dangerous behaviour.

The other issue with sharing specific alerts is that adults will, with the right intentions, focus on the specifics of the story and so may be less open to the signs and symptoms of harm and abuse. The child must be at the centre of our concerns, and if it took a news story to make us take a child self-harming, such as is in the 'Blue Whale' hoax, as a serious concern then we really have to question our own commitment to and understanding of safeguarding.

This hoax/fake issue has happened before, for example:

- Many '**white van kidnapping/abduction'** stories fall into this area. There are frequent social media stories about attempted kidnappings, they spread fast and can result in thousands of shares over a 24-hour period. Often they have no specific location, they are not timed or dated, there is no detail, just fear.
- There was a case involving '**Talking Angela'**, an app where children can hold a text conversation with an animated cat. Stories went round that the app was developed by paedophiles to gain access to children, this was a hoax http://www.thatsnonsense.com/is-the-talking-angela-app-safe-for-kids-we-take-a-look/.
- In August 2013 fourteen year old Hannah Smith committed suicide; the news stories told us Hannah had been bullied on **Ask.fm** https://www.theguardian.com/society/2013/aug/06/hannah-smith-online-bullying. Calls were made to close the site, it was said that the site promoted bullying and suicide; even David Cameron joined in calling for the site to be closed. The Ask.fm site owners stayed quiet – they stayed quiet because they were working with Police, providing facts behind the case. Sometime later, it emerged that the bullying messages Hannah had received were sent from her own computer, she had sent the messages to herself https://www.theguardian.com/uk-news/2014/may/06/hannah-smith-suicide-teenager-cyber-bullying-inquests. This case was not about an evil website, but about the poor mental health of a teenager.

There will always be risk, and stories such as http://www.mirror.co.uk/news/world-news/horrified-parents-warn-paedophiles-using-8363035 'Horrified parents warn paedophiles are using hugely popular musical.ly mobile phone app to groom underage children' – are based in truth, but need to be put into context – every online app with any communication aspect is open to this risk, some are moderated, some have software monitoring, but the risk will always be there. The danger here is that musical.ly is seen as dangerous, but another similar app is seen as safe. The danger in focusing on a particular app is that some parents will ban the app, instead of understanding paedophiles will be there on all apps. Just as if you take children out to a park or a shopping centre, they will be there too. The most important messages are about keeping safe online:

- Follow the age restrictions
- Put privacy settings on
- Don't participate in anonymous chat
- Block, delete and report users or posts that worry you.

Parents should keep the conversation going at home, to talk to their child about what they are doing online. Schools and family at home should celebrate the exciting things and provide sensible advice, caution and support if children are taking risks and report if concerned.

Where there is an alert about a 'real world' situation, such as an attempt to abduct a child, make sure information is specific, timed, dated and located. Offer sensible and ongoing advice to parents and children - children must be aware of their personal safety, tell a trusted adult if they are worried or concerned. Let them know that 999 calls are free from mobile phones and phone boxes.

The risk will always be there, but learning about risk and learning how to manage and mitigate risk is key learning for children and young people. We have to help them with this, and raise concerns where a child is at risk of harm and abuse.

That's nonsense http://www.thatsnonsense.com/ Hoax slayer http://www.hoax-slayer.net/ Snopes http://www.snopes.com/

Click Bait Scams

"Lose 10 pounds in two days! Unmask the latest diet craze that will make you the envy of all your friends!"

"See what this mom did just to get the perfect picture! (Reader caution advised)"

"The number one reason why you should NEVER go on roller coasters with your hair down!"

How many of the above topics sound at least somewhat familiar to you? And how many times have you clicked on similar ones? The implausible and sensational titles are intended to draw readers in and to make them think "I just have to read that one!" That's why even intelligent, thoughtful people might click the link to read that article on why people should never go on roller coasters with your hair down (ouch). And of course you know intellectually that there is just no way to lose 10 pounds in two days (and if there is a way it probably isn't all that intelligent or safe of an option) – But you're just dying to find out anyway.

The above articles are examples of Click bait. Perhaps you have noticed such articles via friends on Facebook or as promoted content links on the bottom of other articles. Sure, they sound crazy and hyperbolic, but just like those tabloids headlines lining the checkout isles they wiggle their way into the curious recesses of your brain, working the same psychological magic as their print counterparts. You click because you just have to know – even though you really do know how preposterous it all really is, leaving your emotions to do the driving while logic takes a back seat.

Click bait – hook, line and sinker.

The real trouble is that click bait is often more than just a simple insult to our intelligence – it can lead to real trouble like malware and scams. Often times clicking on a seemingly-juicy article will lead you to nothing more than a useless pop-up for a fake video player or a fake survey, no article in sight. But if you take the, erm, bait, and download the player or fill in the survey, you'll wind up with a PC full of malware and viruses. In fact, Facebook, well known for sensational and improbable content, started trying to put the brakes on click bait by creating an algorithm to map the time spent on outbound links to determine ones that are real and block the bad ones.

Social media loves click bait

According to a recent report by the Better Business Bureau, news headlines often provide scammers with plenty of click bait-worthy inspiration. For example, last summer's ice bucket challenge to create awareness for ALS spawned a slew of link-based scams. One piece of content making its rounds on Facebook promised to lead readers to a shocking video of an ice bucket challenge gone very wrong. In fact, all it led to was a website with a pop-up for a fake video player, asking to be updated. Viewers who chose to update wound up with a Trojan virus on their computers. This is just one example – there are countless others, like the Facebook post about a guy who pops a black head. From the provocative title you're left to wonder if something gross crawls out – but all you get when you click on the link is sent to a website that asks you to fill out a survey and then steals your identity.

Facebook isn't alone in harboring click bait – you can find it on Twitter and in other places too, even on reputable websites at the end of articles where the Promoted Content articles are – sometimes they are legit, but other times they clearly aren't. The thing that makes social media a hotbed for click bait is that people tend to be trusting and open when it comes to relationships and sharing on these platforms. When you tell everyone what your two-year-old just ate for dinner and about how your dog rolled over and played dead, you're in an open and sharing "groove." In such a state, people become more susceptible and willing to click than they might be with something like a suspicious email – when it comes to email, we all (hopefully) know to be more cautious and judicious. But we feel good and open on social media, and this fuzzy and warm feeling can lead to big-time security issues.

So does this mean you can never click those juicy-sounding articles again?

Well, it certainly means that if you have a propensity to click, click, click away, you need to use more caution than you had in the past. And it also means that you should use more caution in general on social media – approach sharing and opening posts from friends as cautiously as you would your emails. Social media can be a wonderful tool but it can be really dangerous as well and it's beyond important to keep that in perspective. Make sure your antivirus protection is up and running to stay safe from anything you click accidentally and hover over links to see if they lead to a reputable-sounding source or not. If it doesn't sound legit, you can be sure it's not worth the risk. Lastly, resist the urge to know. Keep your wits about you, because you know what they say – curiosity killed the cat. Well, apparently, it's also been known to kill some computers and steal some identities too.

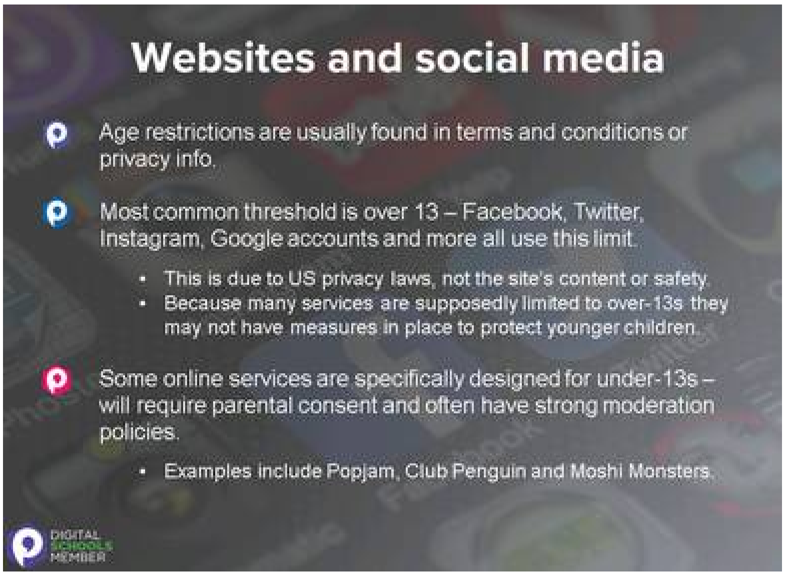
http://www.zonealarm.com/blog/2016/03/click-bait-scams-in-social-media/

Getting to Grips with Age Ratings

Many people already know that lots of social media platforms say they are for 13+ users only, but may not know why. This is down to a US law that requires services collecting data on children under 13 to get parental consent. For simplicity, many such services are now restricted to over-13s only around the world.

If your child does use Facebook or another platform before they turn 13, it's just a term and condition of the site that's being broken – not the law. Many services say they will remove an account if it's proven to belong to someone underage but in practice this can be difficult to enforce and doesn't happen all that often.

Many of these services aren't necessarily inappropriate for under-13s, but because they're intended for older users they may not have the kind of protective tools that would be in place on a site for younger children. There are some online services that specifically cater to under-13s (above), and they often have stricter moderation policies to control user behaviour and regulate the type of content that gets posted.

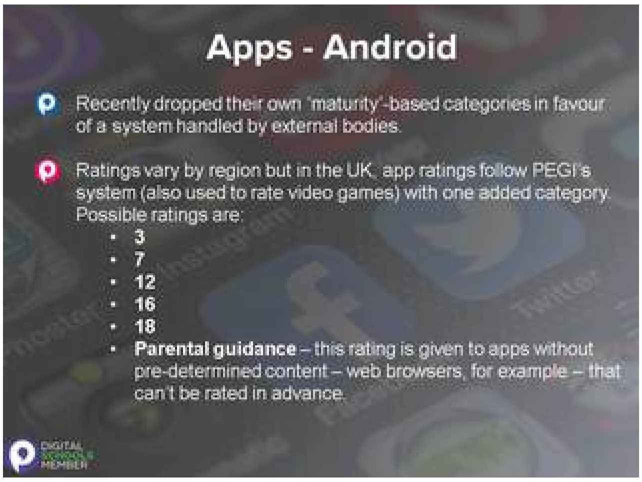


Websites and social media

- Age restrictions are usually found in terms and conditions or privacy info.
- Most common threshold is over 13 – Facebook, Twitter, Instagram, Google accounts and more all use this limit.
  - This is due to US privacy laws, not the site's content or safety.
  - Because many services are supposedly limited to over-13s they may not have measures in place to protect younger children.
- Some online services are specifically designed for under-13s – will require parental consent and often have strong moderation policies.
  - Examples include Popjam, Club Penguin and Moshi Monsters.

DIGITAL SCHOOLS MEMBER

There is no external regulating body (like the BBFC or PEGI) to rate websites and social media based on how appropriate they are for children, so many of your decisions about when your child is ready to use these services will be down to your judgement as a parent. It's not a bad idea to familiarise yourself with some of the sites your child wants to use so you can make informed decisions.



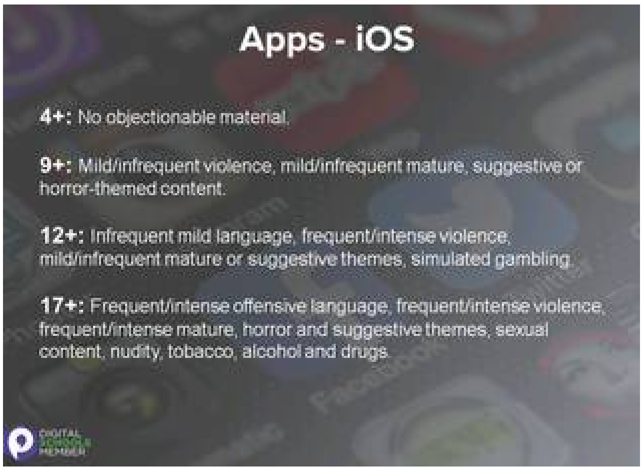
Apps - Android

- Recently dropped their own 'maturity'-based categories in favour of a system handled by external bodies.
- Ratings vary by region but in the UK, app ratings follow PEGI's system (also used to rate video games) with one added category. Possible ratings are:
  - 3
  - 7
  - 12
  - 16
  - 18
  - **Parental guidance** – this rating is given to apps without pre-determined content – web browsers, for example – that can't be rated in advance.

DIGITAL SCHOOLS MEMBER

Until recently, Android apps received one of four ratings based around an app's 'maturity' level – they weren't technically age ratings because the categories didn't come with a suggested age. This rating system was applied across the board in all regions.

Android apps have now moved to a system in which the International Age Ratings Coalition (a coalition of age rating bodies, like Europe's PEGI) assign appropriate age ratings as measured locally. In the UK, for example, apps are assigned one of the age ratings already used by PEGI to classify video games – 3, 7, 12, 16 or 18 (more on this system later).



Apps - iOS

4+: No objectionable material.

9+: Mild/infrequent violence, mild/infrequent mature, suggestive or horror-themed content.

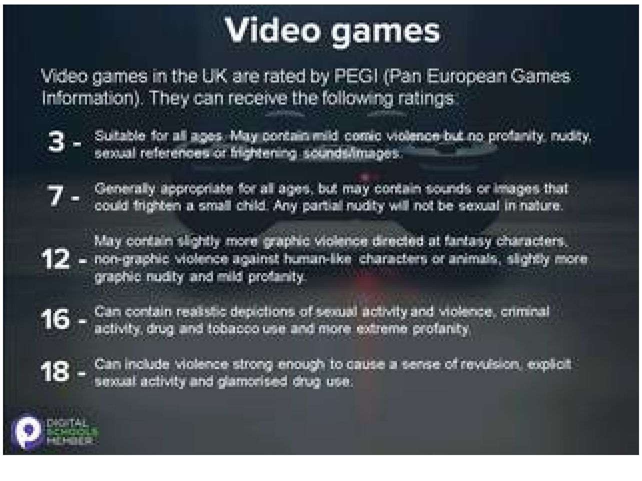
12+: Infrequent mild language, frequent/intense violence, mild/infrequent mature or suggestive themes, simulated gambling.

17+: Frequent/intense offensive language, frequent/intense violence, frequent/intense mature, horror and suggestive themes, sexual content, nudity, tobacco, alcohol and drugs.

DIGITAL SCHOOLS MEMBER

One additional category has also been added – parental guidance. Because many apps act as a portal to other content, it's not possible to say in advance how appropriate the content will be for children. If an app receives the parental guidance rating, it means content varies and parents should use their judgement to decide if the app is appropriate.

iOS apps (apps for Apple devices) are age rated according to the system above. Like many other age rating systems, these categories refer to appropriateness of content only and not general suitability. An app rated 4, for instance, isn't necessarily designed for children – it just contains nothing specifically inappropriate for them.



Video games

Video games in the UK are rated by PEGI (Pan European Games Information). They can receive the following ratings:

3 - Suitable for all ages. May contain mild comic violence but no profanity, nudity, sexual references or frightening sounds/images.

7 - Generally appropriate for all ages, but may contain sounds or images that could frighten a small child. Any partial nudity will not be sexual in nature.

12 - May contain slightly more graphic violence directed at fantasy characters, non-graphic violence against human-like characters or animals, slightly more graphic nudity and mild profanity.

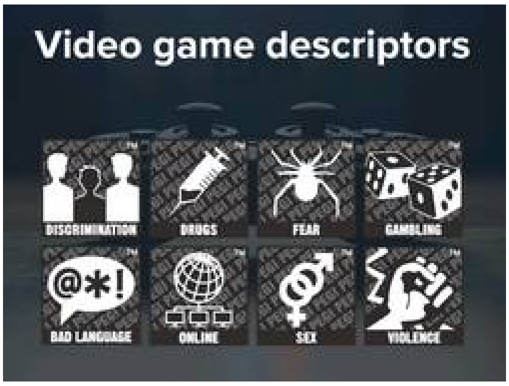
16 - Can contain realistic depictions of sexual activity and violence, criminal activity, drug and tobacco use and more extreme profanity.

18 - Can include violence strong enough to cause a sense of revulsion, explicit sexual activity and glamorised drug use.

DIGITAL SCHOOLS MEMBER

Since 2012, PEGI ratings for video games have been legally enforceable in the UK. Games receive a rating from 3 to 18. The 3 and 7 ratings are only advisory, but 12, 16 and 18 are mandatory and it is illegal to sell a game with one of those ratings to someone under the specified age.

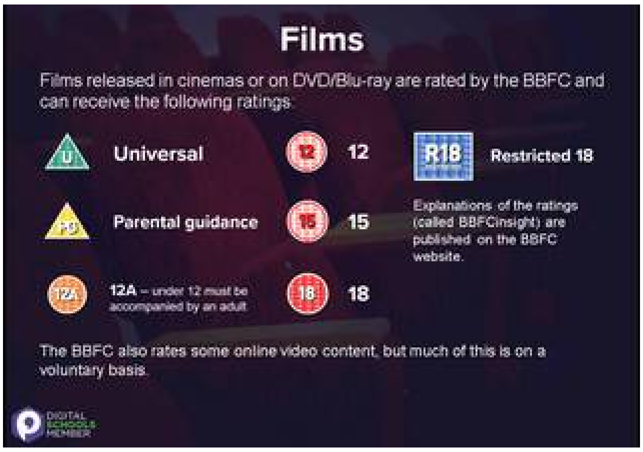
The ratings are explained above.



Video game descriptors

Because there are several different factors that can justify a video game's age rating, the ratings are normally accompanied by explanatory descriptors.
Descriptors should be interpreted in the context of the age rating, since the same descriptor can justify different ratings depending on the severity. So it would be possible for, say, a 12 rated game and an 18 rated game to both have violence descriptors – but the content would be much more extreme in the 18 rated game than the 12 rated game.

These descriptors are a useful tool to figure out whether a game is appropriate for your child. Children mature at different rates and everyone is sensitive to different things, so knowing whether a game's rating is because of, say, fear or sexual content might help you decide whether your child is ready to play it – even if they're technically old enough.



Films

Films released in cinemas or on DVD/Blu-ray are rated by the BBFC and can receive the following ratings:

U Universal

PG Parental guidance

12A 12A – under 12 must be accompanied by an adult

12 12

15 15

18 18

R18 Restricted 18

Explanations of the ratings (called BBFCinsight) are published on the BBFC website.

The BBFC also rates some online video content, but much of this is on a voluntary basis.

These are the ratings that the BBFC uses to classify film content in cinemas, on DVD and Blu-ray. Increasingly online video is also receiving BBFC ratings (though this is by no means universal) – a list of online services that use BBFC ratings can be found here: http://www.bbfc.co.uk/what-classification/digital-age-ratings
Because there are so many different types of video content, there are lots of different things that can justify a film's age rating. To help you, the BBFC publishes an explanation of the rating for each film they review – called BBFCinsight. More information here: http://www.bbfc.co.uk/what-classification/what-bbfc-insight

Brief explanation of the categories:

- U – stands for universal. Films in this category should be appropriate for anyone over age 4.
- PG – stands for parental guidance. These films are appropriate for general viewing but might have some scenes that are unsuitable for young children – so as the name suggests, parents should use their judgement to decide whether a PG film is suitable for their individual child.
- 12A and 12: these films contain material that may not be suitable for children under 12. The 12A rating means that no one under 12 is allowed to see one of these films in a cinema unless they are accompanied by an adult. Films rated 12A in cinemas will have a 12 rating on DVD and blu-ray, because it's not possible to enforce adult accompaniment at home. Adults are allowed to take children to 12A films, but the BBFC recommends reading more about the film in advance to see if it's appropriate for the child.
- 15: films with this rating are not considered suitable for children under 15. Under-15s are not allowed to rent or buy films with this rating or see them in the cinema, even with an adult.
- 18: films with this rating are for adults only (i.e. over 18s). Children cannot buy, rent or view them in a cinema, even with an adult.
- R18: films with this rating are for adults only and can only be shown in specially licensed cinemas. Often they involve explicit sexual or fetish content.

More information:
http://parentinfo.org/article/how-old-do-you-have-to-be

Support sites

UK safer internet centre https://www.saferinternet.org.uk/

LGfL Online Safety http://os.lgfl.net

Childnet http://www.childnet.com/

NSPCC https://www.nspcc.org.uk/

Parentzone https://parentzone.org.uk/

parent INFO
FROM CEOP AND PARENT ZONE

6 apps that every parent should know about + boys & body image + tips for parents struggling to make ends meet + the 'Am I pretty?' video craze + more *http://parentinfo.org/article/the-6-apps-and-services-that-every-parent-should-know-about*