School Improvement
Liverpool

October 2021
paul.bradshaw@si.liverpool.gov.uk
@silesafety

Online Safety Update

FAO Headteachers, Designated Safeguarding Leads
& Computing Subject Leaders

Welcome to issue 33 of the Online Safety Update brought to you by School Improvement Liverpool.

This update is for leaders and practitioners working with children and young people in schools and other settings across Liverpool.

The aim is to bring you relevant information to assist you in educating children and young people about how to keep themselves safer when using the internet and social media and for you to give them an increased awareness of digital risks.

If you would like to access the resources/documents referenced in this update, you can locate them by visiting this link: http://bit.ly/OS2122 - here you will also find archive issues of this newsletter

You can also visit - https://www.schoolimprovementliverpool.co.uk/onlinesafety

I hope that the new academic year has started well in your school. I just wanted to use this update to highlight some of the online safety themes I shared during the recent round of Annual Headteacher Safeguarding Briefings.

Keeping Children Safe in Education – September 2021

The main Online Safety references in KCSIE can be found in **paragraphs 123 – 135**, together with complementary **Annex D** (Annex D contains a wealth of additional information to support schools and parents to help keep children safer online and is reproduced in full at the end of this update).

123. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

An important changes come in paragraph 124 in relation to ***Commerce*** *–*

124. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (eg consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Commerce thus becomes the fourth C. Since the Byron Review (Safer Children in a Digital World, 2008) there have previously only been three Cs. (If you are interested, you can access the Byron Review via the link at the start of this update).

126. Online safety and the school or college's approach to it should be reflected in the child protection policy. **Considering the 4Cs (above) will provide the basis of an effective online policy.** The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect in their mobile and smart technology policy and their child protection policy.

Filters and monitoring

128. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, **governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.**

129. **The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty**. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring.

The UKCIS documents can also be found at the link at the start of this update and I would encourage you to read them especially in light of the following news story.

Frankie Thomas: Girl who died could 'view anything' on school iPad – 13/07/21

https://www.bbc.co.uk/news/uk-england-surrey-57825879

The web filter at a school where a girl took her own life after viewing graphic content failed so badly she "could view anything", an inquest heard.

Frankie Thomas died at her home in Witley, Surrey, in September 2018.

The 15-year-old's browsing history revealed she had been accessing self-harm images for months.

The former business manager of Stepping Stones school, in Hindhead, said he believed the filter was working, but later discovered it was not.

Former business manager Isaac Xenitides, who joined four months before her death, told the hearing in Woking he was led to believe a filter for the entire school network was in place and working.

Only later he found out it had "not been set up properly in the first place".

He said he wanted to find out "how a filter could fail so badly", meaning that "children could view anything".

He also told the court the school appeared to be aware of problems with the internet filtering system in the year before Frankie died.

The inquest also heard from David Cross, who took over as the school's network manager in 2019.

He said he also found the internet filter were still not "sufficient" or "adequate".

Music teacher Ben Bastin told the hearing he thought the iPads at the school were subject to filtering software, and he would also try to observe Frankie's use of the devices by "looking over her shoulder".

The court heard if he had known the filtering system did not work on iPads, no student would have been allowed unsupervised access.

My advice to schools…

1. Read the UKSIC documents

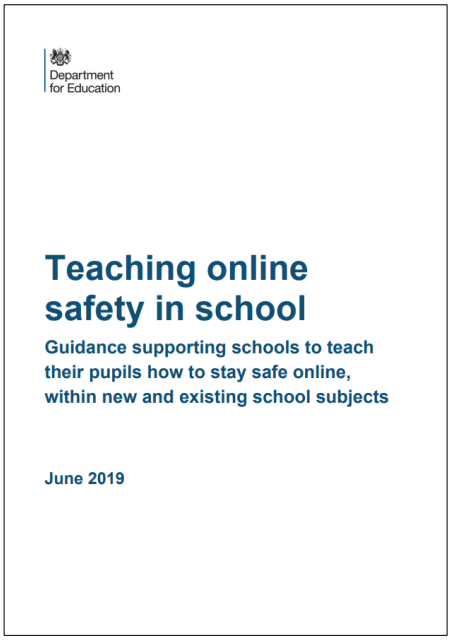
2. Carry out an Appropriate Filtering & Appropriate Monitoring Risk Assessment with a governor(s)

3. Document your Risk Assessment and your school's approach to Appropriate Filtering & Appropriate Monitoring

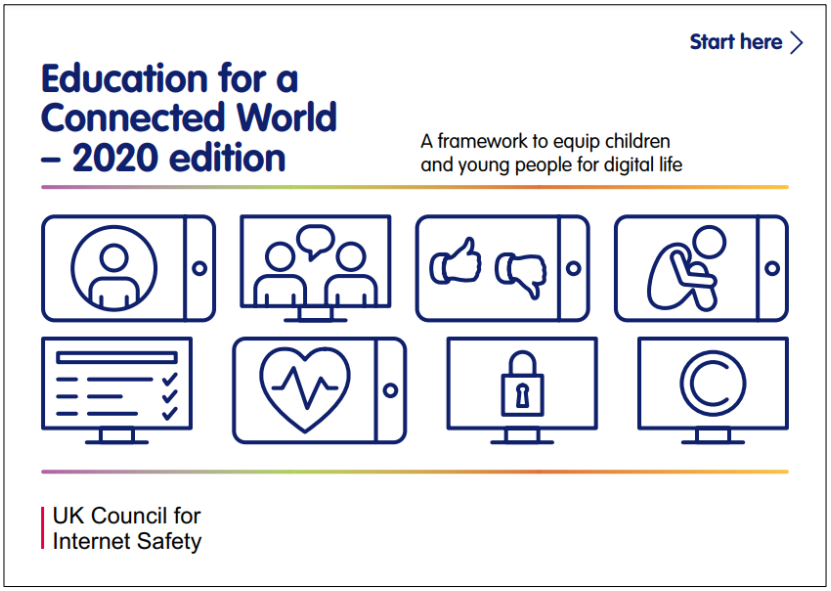
4. Share with Full Governing Body

(Also check out Bedtime Stories videos from https://www.papyrus-uk.org/bedtime-stories/bedtime-stories-chapter-two/)

Three **FREE** resources, referenced in **KCSIE Annex D**, worth re-visiting at again…



1.



2. (Suitable for all schools, covers ages 4-18)

3. **Project Evolve** - https://projectevolve.co.uk/ - this builds on the themes in "Education for a Connected World" and provides a range of lesson plans and other activities.

London Grid for Learning Online Safety Policy & Acceptable Use Policies

As you may already know, Liverpool is a partner member of the London Grid for Learning. Over the summer months, the LGfL DigiSafe team (including contributions from myself) have updated their Online Safety Policy and AUPs to take into account the latest version of Keeping Children Safe in Education. All Liverpool schools can access these policies which are available at the bit.ly/OS2122 link and at…

https://www.lgfl.net/online-safety/resource-centre?s=24

Internet Watch Foundation "Home Truths"

https://talk.iwf.org.uk/

Are you unknowingly letting child sexual abusers into your home?

Young people are being contacted in their own homes on online platforms and apps and asked for sexual pictures and videos, while their parents and carers believe they are safe.

More and more sexual abuse material is created by offenders who coerce and groom children into sexual activities, often in children's own bedrooms and bathrooms. They then record this via webcams or livestreaming services. It's known as 'self-generated**' child sexual abuse imagery.

This is happening now, and it can happen to anyone. But you can do something about it; you can help prevent it happening to your child.

There is a powerful video that accompanies this campaign that you may want to use with parents/carers.

https://www.youtube.com/watch?v=OlCELNnd98o&t=16s

Ofcom – Media Nations 2021 – August 2021

This is an interesting read – probably best to just search for "children" if you don't want to read the entire document.

Did you know, for instance, that Netflix is the most popular online video platform among 3-17 year olds, ahead of YouTube.

..and that Netflix is also the leading video on demand platform, by content streams, followed by BBC iPlayer… 5.5 billion streams vs 1.7 billion streams (Q1 2021)

Teacher Regulation Agency – Prohibition Orders

Just to flag with you that over the past four years **275*** teachers have received a Prohibition Order for the misuse of social media/technology.

In relation to this can I just remind you of KCSIE paragraphs…

84. Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare.

85. This should include:

a staff behaviour policy (sometimes called the code of conduct) which should amongst other things, include - acceptable use of technologies (including the use of mobile devices), staff/pupil relationships and communications including the use of social media.

(*275 as of 29/09/21)

Safer Internet Day – Tuesday 8th February 2022 – save the date!

https://www.saferinternet.org.uk/safer-internet-day/2022

Finally, if you need any advice or support relating to Online Safety matters in your school or setting, please do not hesitate to contact me, I will always do my best to assist.

Paul Bradshaw - Senior School Improvement Officer - New Technologies & Online Safety

Annex D: Online Safety

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's

personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

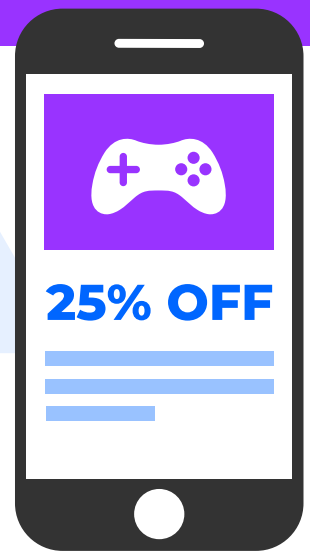
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world

- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

How to protect young people from social scams

internet matters.org

In partnership with BARCLAYS



Talk to children about the issue using news stories to start conversations

- When there is a story in the news about the latest online scam then **share this with the whole family** – don't just target young people as anyone can be affected by these things and the more we talk about online issues the more natural and normal it will become!

Encourage young people to check their privacy settings on their social media accounts

- **Most social media platforms and popular apps are public by default**, but most will allow users to control their privacy for example choosing who can see their content or who can contact them. You can find information on how to access these privacy settings here. Once the privacy settings are in place it is still important to remind children and young people to think carefully before sharing too much information.

Encourage young people to be more critical about the ads they see on social media

- Adverts on social media will often look genuine and encourage you to click to visit their website to make a purchase, **it is especially important to make sure that you are on the site that you think you are on.** If in doubt, then browse to the site yourself rather than relying on a link in the advert. Also, have a read of our online critical thinking guide to help young people learn how to make smarter choices online.

If you are in any doubt about whether an offer or a post is genuine then visit the website yourself

- **Encourage young people not to click on any links in a social media post or email** – type in the address, login if necessary and see whether the offer or claim is indeed genuine.

Reinforce the importance of protecting personal data

- **Remind young people that their bank will NEVER ask them to provide online banking password details** or a One-Time-Passcode if they are using two-factor authentication via an email or social media platform, nor will their bank ever ask them to transfer funds to a safe account or say their money is at risk.

Always report if something looks like a scam

- If you or your children become aware of something that looks suspicious online, then it is important to act. **Report it to the platform** (you can find out how to do that here) and you can also report to Action Fraud. Action Fraud is the UK's national reporting centre for fraud and cybercrime and is the place where we should report scams if we live in England, Wales, or Northern Ireland. In Scotland this can be reported directly to the police.