In this issue:
- The dangers of 'hackable' toys
- Online safety & engaging parents
- Sadfishing
- Online Safety Conference 2020
- Horizons - Maintaining wellbeing
Welcome
Here's your latest issue of the Online Safety Newsletter for Spring 2020. Please feel free to share this newsletter with other members of staff from your school. We hope you find the newsletter useful and if you have any feedback about our service to schools or if there is anything you would like to see in next term’s update, please get in touch - vikki.bardon@entrust-ed.co.uk.

Preparing for the change yet? Will you be ready for September 2020?

Some schools have already adapted their online safety curriculum in light of the statutory changes for Relationships Education, Relationships and Sex Education (RSE) and Health Education. PSHE and Computing leads have joined forces to map out online safety provision across the school to cover the requirements – has your school started this yet?

Some of the early adopter schools have already attended our Horizons series - Maintaining Wellbeing in a Digital World and it’s not too late for you either.

We are changing the delivery model and are running two of the three sessions on the same day – you can attend both or just one, each session to attend is £75 (lunch is not provided).

4 March 2020, 09:30 – 12:15
Fort Dunlop, Erdington, Birmingham, B24 9FD
Session 1: ‘Coping with the pressures of an online life’

4 March 2020, 13:00 – 15:30
Fort Dunlop, Erdington, Birmingham, B24 9FD
Session 2: ‘An ecological approach to mental health and behaviour’

12 March 2020, 09:30 – 12:15
Entrust HQ, Riverway, Stafford, ST16 3TH
Session 1: ‘Coping with the pressures of an online life’

12 March 2020, 13:00 – 15:30
Entrust HQ, Riverway, Stafford, ST16 3TH
Session 2 ‘An ecological approach to mental health and behaviour’

Click here to register at our Birmingham training centre.
Click here to register at our Stafford training centre.

DfE publication - Teaching Online Safety in School

In June 2019, the DfE released non-statutory guidance called Teaching Online Safety in Schools which is packed with really useful guidance and ideas to shape your changes to online safety. This document is referred to in the statutory document Keeping Children Safe in Education and Ofsted have been known to refer to its content during deep dive inspections for safeguarding and computing. If you are not aware of the content
Sadfishing

Vulnerable young people who go online to seek support can find themselves being bullied and accused of “sadfishing.” The term refers to the act of posting about a personal problem online to gain support or understanding from followers in the form of likes and comments. While there will be some cases where young people will persistently share exaggerated posts to gain sympathy, we need to be cautious with dismissing these behaviours as ‘attention-seeking’.

Sadfishing evolved as a term after celebrities, such as the reality star Kendall Jenner, were accused of posting exaggerated claims about their problems in order to gain attention and followers on social media.

Digital Awareness UK (DAUK) is concerned about the number of students who are bullied for sadfishing (through comments on social media, on messaging apps or face-to-face), thus exacerbating what could be a serious mental health problem. DAUK have noticed that students are often left feeling disappointed by not getting the support they need online.

There are also concerns around vulnerable youngsters being targeted by groomers who prey on them by providing sympathy and sharing their own experiences in order to gain their trust.

Who are your vulnerable pupils and what is provided to them in the way of additional online safety support?

It’s important that young people are able to talk about how they feel, and some will seek support

ProjectEVOLVE – free resources

If your school is not using Education for a Connected World framework then why not? Not only does the framework cover 8 themes for online safety with 330 progressive learning statements from Year 1 through to Year 13, there is now another reason for using the framework. ProjectEVOLVE Toolkit resources each of the 330 statements providing outcome criteria; questions to ask; activity descriptor and resources.

Currently 4 of the 8 themes are populated in the toolkit with the other 4 areas coming soon.
online from close friends. However, oversharing publicly could be counterproductive for some young people and could make them feel even more vulnerable and overexposed.

If a child in your care engages in so-called "sadfishing" it's an indication that you need to check in with them and offer some support – read this article to find out how you can help.

**Facebook’s Content Moderation Report**

In November 2019, Facebook released its latest content moderation report and it makes for a compelling read.

Between April and September, Facebook Inc removed:

- 3.2 billion fake accounts
- more than 11.6 million pieces of content depicting child nudity and sexual exploitation of children on Facebook and 754,000 pieces on Instagram
- 2.5 million posts that depicted or encouraged suicide or self-injury
- 4.4 million pieces involving drug sales

Facebook plans to provide greater privacy to users by encrypting the company’s messaging services. Law enforcement is concerned that this will hamper efforts to fight child abuse and that the changes would turn the platform into a “dream come true for predators and child pornographers.”

**Teen’s TikTok video about China’s Muslim camps goes viral**

A recent BBC news report describes how a US teenager’s TikTok video accusing China of putting Muslims into “concentration camps” went viral. The post appears to be about beauty tips at its start - but the young woman then changes tack to ask her viewers to raise awareness of what she describes as a “another Holocaust”. It had been watched more than 1.4 million times and “liked” nearly 500,000 times on the app. A copy uploaded to Twitter by other TikTok users has attracted a further five million views.

TikTok permanently banned one of the teenager’s accounts as it had broken the rules. However, TikTok does not moderate content due to political sensitivities. Although, Douyin, the Chinese version of the app, on which Ms Aziz’s posts would not have appeared, is politically censored.

TikTok has now lifted the ban, maintaining it was due to 17-year-old Feroza Aziz’s prior conduct on the app - and unrelated to Chinese politics.

**Did you know** that when TikTok bans users, it also prevents the same device being used to set up another account?
TikTok changes virtual gifts policy after BBC probe

In July last year, the BBC revealed how children and teenagers were being pressured to buy digital items for “celebrities” on the platform. In some cases, fans bought gifts worth hundreds of pounds - which could be swapped back for cash - in exchange for phone numbers and private messages. The updated policy (December 2019) only allows those aged 18 and over to purchase, send, or receive virtual gifts.

The Internet of Things – how to use everyday objects that connect to the internet safely in your home

Playing with the latest robotic toy or talking to a smart speaker, our homes have become even more connected. Industry experts have predicted that there will be over 20 billion connected devices in our homes worldwide by 2020. Although connected devices and toys provide children with opportunities for learning and interactive play, there are risks associated with the Internet of Things:

- Concerns have been raised about whether these devices are collecting too much personal information from children
- Some children (either accidentally or on purpose) are able to search for and access age-inappropriate material via a connected device such as a smart speaker
- Children may make ‘in-app purchases’ and spend money, which is often taken from their parents’ bank account without their knowledge or consent
- Some of these devices may be more vulnerable to hacking and monitoring, as there are currently no security standards in place for connected devices

Read the article to discover how you can minimise these risks.

'Hackable' karaoke and walkie talkie toys found by Which?

A walkie talkie toy and two karaoke devices have been found to be potentially hackable, consumer group Which? has claimed.

The toy’s Bluetooth connections were tested by Which? and cyber-security firm NCC Group. They found a nearby stranger could potentially talk to children via the devices. Vtech, which made the walkie talkie, said new connections could not be made if a parent’s device had already been paired with the toy.

Three out of seven popular toys examined during tests were found to have flaws, meaning a stranger could, under certain conditions, speak to children
via the devices. A stranger could, for example, use a Vtech’s KidiGear walkie talkie to pair to another KidiGear device being used by a child - from a distance of up to 200m (656ft). The Bluetooth pairing of devices, however, would have to take place within a 30-second window, once the child’s device was activated. “Based on all this information we have gathered, we believe that there is a risk of someone observing a child playing with the walkie talkies and exploiting the above scenario,” said Which?

Which? also found that the Singing Machine SMK250PP karaoke machine had been designed so that a stranger could stream audio to a child from a distance of up to 10 metres because the Bluetooth connection did not ask for authentication. “So as long as the machine is on and is listening for Bluetooth connections, it will happily connect with any Bluetooth streaming device that initiates communication with it,” said Which?

The Internet Matters guide to tech: Buying a smart toy is a resource worth sharing with parents and carers.

Three ways to engage parents and carers with online safety

Getting parents involved in your online safety education can be challenging but don’t give up, parental engagement is crucial in making sure children receive consistent online safety messages at home.

1. Run a workshop – struggling with attendance? Have you tried running a session before a parents’ evening; during an open-evening and transition event; class assemblies, presentations and school productions; immediately before/after drop-off or pick-up or maybe record the session as a webinar and post on your website.

2. Share advice on your socials – use your newsletters and social media channels.

3. Keep your website updated with the latest online safety news and articles – embed ParentInfo in your website, provides easy access to up-to-date articles with advice for families in a digital world. Register your organisation to find out how you can embed the content in three easy steps.

Snapchat Cameos

Snapchat has launched its big new feature that uses your selfies to replace the faces of people in videos you can then share. It’s essentially a simplified way to deep-fake you into GIFs. Snapchat Cameos are an alternative to Bitmoji for quickly conveying an emotion, reaction or silly situation in Snapchat messages.

Does this new feature normalise creating deepfakes?
‘Into the Cloud’ from NetSmartz

Join Nettie and Webster on an adventure through the digital cloud where you’ll have to put everything you’ve learned about online safety and digital citizenship to the test!

Online Safety themes addressed in Into the Cloud: Cyberbullying; Online Privacy; Online Enticement; Unreliable Online Information; Inappropriate Online Content and more!

Episodes 1 and 2 “Enter Badromeda” and “T.M.I.” (too much information) looks at not responding to the taunts and drama they may encounter online and understanding why online privacy is important.

Episodes 3 and 4 “Rocket Bike” and “Fact or Fake?” tackles the issues of cyberbullying, bystanders, and upstanders, and the dangers of online distractions!

Episodes 5 and 6 “Checking In” and “Finding Vera”. focus on what to do if kids find content online that makes them feel sad, scared, or confused, and dive into the issues of digital grooming and luring is now available to download or stream at NetSmartzKids.org

Resources to help keep young people safe while gaming

Many children will have had new games consoles, devices and online subscriptions to purchase games, so how does your online safety curriculum cover safe gaming to enable young people to benefit from the opportunities of online gaming as well as develop the skills to respond safely to risks? Here are three resources you could build into your curriculum:

Jessie and Friends episode 3 resource for 6-7s to understand the importance of keeping personal information safe; identifying and responding safely to manipulative behaviour; know how to seek help from an adult they trust.

Play, Like, Share (updated 2019) resource pack to help 8-10s to identify signs of abusive behaviour they may come across on gaming platforms; responding safely if they think someone is trying to manipulate, pressure or threaten them; get help from an appropriate source if they need it.

Gaming or gambling? Gambling-like behaviour is woven into gaming. Sign up to download your free pack designed to help professionals and families learn about gambling-like risks children may face when playing online games.

‘Gaming’ and ‘Online gaming: tips for playing safe’ for 11-14+ as a way to start important conversations with young people.

To support parents and carers, CEOP have a comprehensive section on their website regarding gaming.
Google Stadia

In November 2019, Google launched a cloud service that lets you play big-budget games without discs or downloads, consoles or gaming PCs. Stadia lets you stream the games you buy on servers in the cloud. All you need is a decent internet connection, a good Wi-Fi router, a Stadia Controller and your pick of Google's Chromecast Ultra dongle, Pixel phone, or the Chrome web browser on a laptop or desktop. It’s effectively a beta that Google is charging real money for, and you should wait until 2020 for that to change when Stadia will become a free service, plus the cost of games.

How many of your pupils are aware of Google Stadia or have paid to be an early adopter of the technology? Maybe one to tell parents about particularly as the cost can be avoided if they wait a little longer AND as games consoles are not required, could young people be playing games without the knowledge of their parents for hours on end? For further information on Google Stadia, read this article.

Google Be Internet Legends

Google updated its resource pack ‘Be Internet Legends’ and it now contains more lessons and ideas than before. Download your updated packs here.

Google’s new Digital Wellbeing module

Designed to help Key Stage 2 pupils (7 to 11-year-olds) learn about how their use of technology can make them feel – and reflect on what a healthy balance looks like. Order the FREE resource here.

Making Choices: Sex, Relationships and Age Ratings

A new secondary resource created by the BBFC and the PSHE Association to teach students the skills needed to make considered and informed choices about the content they watch, coping with peer pressure and recognising the differences between real life and on-screen relationships. There are three lesson plans, a teaching guide and extension activities.
Online Safety in the Primary Curriculum

This half-day training course will examine the requirements of the online safety elements of the curriculum at Key Stages 1 and 2 and link this to a range of resources allowing staff to plan an appropriate scheme of work for their school.

18 March 2020, 13:00 – 15:30  
Entrust HQ, Riverway, Stafford, ST16 3TH  
Booking code: LTLT-0320-T001

18 March 2020, 13:00 – 15:30  
Fort Dunlop, Erdington, Birmingham, B24 9FD

28 April 2020, 13:00 – 15:30  
Entrust HQ, Riverway, Stafford, ST16 3TH  
Booking code: LTLT-0420-T001

29 April 2020, 09:30 – 12:00  
Fort Dunlop, Erdington, Birmingham, B24 9FD

Online Safety for Designated Safeguarding Leads

This course is designed for DSLs to understand the role of online safety in line with the expectations from ‘Keeping children safe in education’, “The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).” The course will cover:

- Reviewing government policy and guidance
- Risks and issues to young people
- Review Online Safety curriculum and whole school strategies
- Self review and benchmarking tools to assess your schools provision
- Risks and issues for adults working with young people

21 May 2020, 09:30 – 15:30  
Entrust HQ, Riverway, Stafford, ST16 3TH  
Booking code: LTLT-0520-T001

8 June 2020, 09:30 – 15:30  
Fort Dunlop, Erdington, Birmingham, B24 9FD

Online Safety Conference 2020

Don’t miss out on what is set to be an informative day, presenting an opportunity to gain information that can support your school. You can build on your existing practices or we can point you in the right direction in your online safety provision, within the safeguarding agenda.

There will be leading experts from several areas of online safety. ChildNet will be delivering a presentation on ‘Online Identity’. This session will look at how offline stereotypes, like discrimination are challenged or reinforced, does the internet allow young people to experiment and express themselves, or do they feel limited in who they
can be online? It aims to inspire young people to support each other in being who they want to be and there will be an opportunity to discuss the classroom resources available to support you in school.

This is a **FREE event** but places are limited. If you have not registered your place(s) yet, then please make your booking without delay:

**Wednesday 29 January 2020**  
The Pavilion, Moor Lane, Birmingham B6 7AA  
[Register now](#)

**Thursday 30 January 2020**  
Entrust HQ, Riverway, Stafford, ST16 3TH  
**Booking code:** LTTL-0120-T005  
[Register now](#)

**Tuesday 4 February 2020**  
West Sussex Hilton Avisford Park, Arundel Hotel, Yapton Lane, Walberton, Arundel BN18 0LS  
[Register now](#)

---

**We are here to help**

If you require any in-school support, please do get in touch, we will do all that we can to help.

**Stafford**  
Email: [lt@entrust-ed.co.uk](mailto:lt@entrust-ed.co.uk)  
Call: 0333 300 1900

**Birmingham**  
Email: [info@link2ict.org](mailto:info@link2ict.org)  
Call: 0121 303 5100

**West Sussex**  
Email: [edtech@entrust-ed.co.uk](mailto:edtech@entrust-ed.co.uk)  
Call: 01243 777300
Birmingham Office
5th Floor, Fort Dunlop
Erdington
Birmingham
B24 9FD
Tel: 0121 303 5100
Email: servicedesk@link2ict.org

Stafford Office
Entrust Riverway Centre
Riverway
Stafford
ST16 3TH
Tel: 0333 300 1900
Email: It@entrust-ed.co.uk

West Sussex Office
County Hall
West Street
Chichester
PO19 1RG
Tel: 01243 777300
Email: edtech@entrust-ed.co.uk