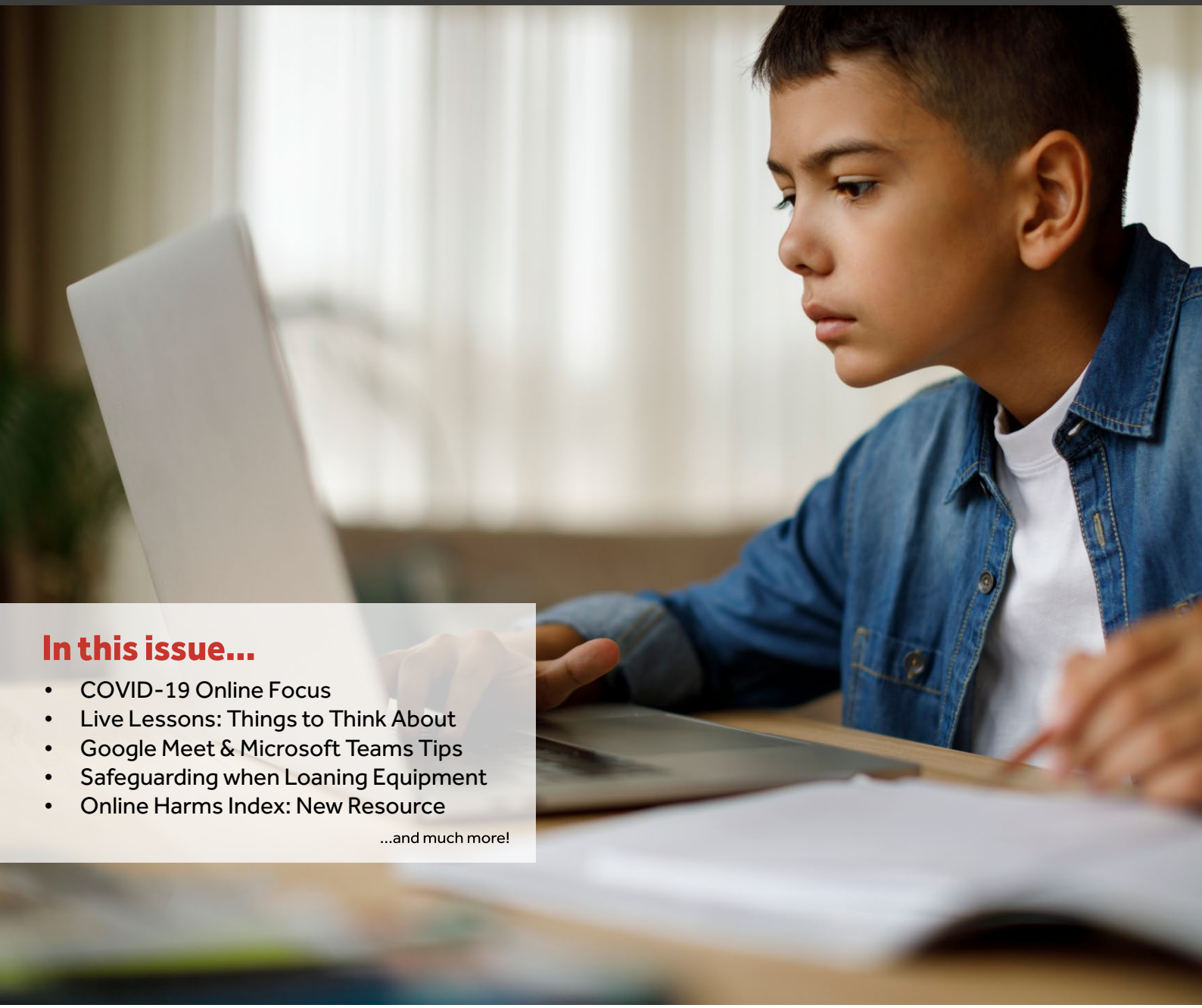
Online Safety Newsletter

Entrust Education Technologies

Autumn 2020



In this issue...

- COVID-19 Online Focus
- Live Lessons: Things to Think About
- Google Meet & Microsoft Teams Tips
- Safeguarding when Loaning Equipment
- Online Harms Index: New Resource

...and much more!

Call **0333 300 1900** Email **edtech@entrust-ed.co.uk**
or visit **www.entrust-ed.co.uk** to find out more about our services.

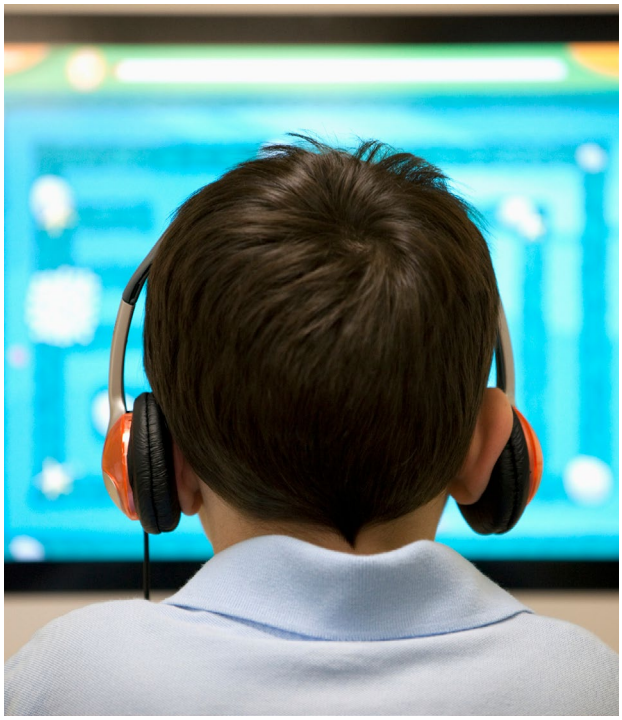
Entrust Education Improvement Entrust Support Services Limited @entrustEDU

entrust
Education Technologies

Welcome

Hope you are all keeping safe and well. This term's newsletter will begin with a few special features covering items related to online safety and the issues schools are dealing with due to COVID-19, then will follow the general style of points to note in the general online safety arena.

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 anything you would like to see in next term's update, please do not hesitate to let me know by emailing vikki.bardon@entrust-ed.co.uk



COVID-19 Online Focus

Are your remote workers at risk of a ransomware attack?

A recent report found that ransomware attacks surged by **72%** since the switch to remote working. It is important that your staff are prepared and know how to detect and respond to security threats when working from home.

Rise in the number of cybercrime attacks on schools, colleges and universities

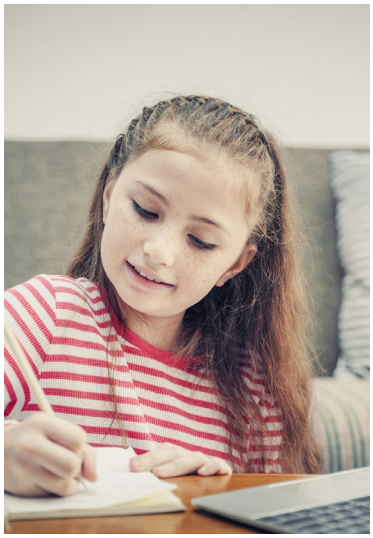
The National Cyber Security Centre raised an alert on 17 Sept to warn of these increased attacks and have updated their guidance for mitigating malware and ransomware.

"Our Cybercrime and Threats – how safe is your data?" staff session is now offered remotely to schools. If you would like to know more about what is covered during this cyber security risks session or to arrange a remote session, please get in touch vikki.bardon@entrust-ed.co.uk

Gaming Soared During Lockdown

Support parents and carers with keeping young people safe when playing online. Research shows only 1 in 3 parents check age ratings. Share the Internet Matters parental control how-to guides on how to set the right level of protection on the gaming consoles, platforms and apps to give young people a fun and safe experience.

Live Lessons
Things to think about...



In these ever-changing times that we find ourselves, increasingly, schools are utilising technology to support distanced/blended learning.

The Education Endowment Foundation has examined existing research for approaches that schools could use, or are already using, to support the learning of pupils remotely, access to technology is key.

A summary of the findings can be found here:
EEF Rapid Evidence Assessment – Distance Learning Summary

If your school is moving to or utilising live lessons, please reflect to see if the following steps have been taken:

Steps to Live Lessons:

- **Policies updated** to include guidance and behaviour guidelines for distance learning - think about this in terms of students, staff and parents.
- **Connectivity** and access to devices – identify what students will have access to. Many children will not wish to hold a hand high to declare they don't have access, try using an online survey. Drill down to find out type of device and if that device is a shared device. Microsoft Forms and Google Forms are excellent for this and free.
- **Platform** – decide on what platform you will use for live lessons e.g. Microsoft Teams or Google Meet. Avoid using live streaming social media tools.
- **Recording** – decide if recordings or live lessons will be made. Many schools consider the recording of lessons an effective tool to capture an audit trail of the lesson, however explicit consent to record lessons should be sought to comply with data protection. Think about where and how that data will be stored securely, how long any recordings are stored for, and when and how they will be removed. They are helpful to allow for lessons to be revisited by students. If they are under the age of 13, only parents or Guardians can give consent.
- **Carry out a risk assessment** and address any issue that have been highlighted, including a Data Protection Impact Assessment (DPIA)
- **Consult** with your designated safeguarding lead and your data protection officer, to ensure you have all the right safeguarding measures in place.

0333 300 1900 | edtech@entrust-ed.co.uk | www.entrust-ed.co.uk

Google Meet and Microsoft Teams
Online Safety Tips

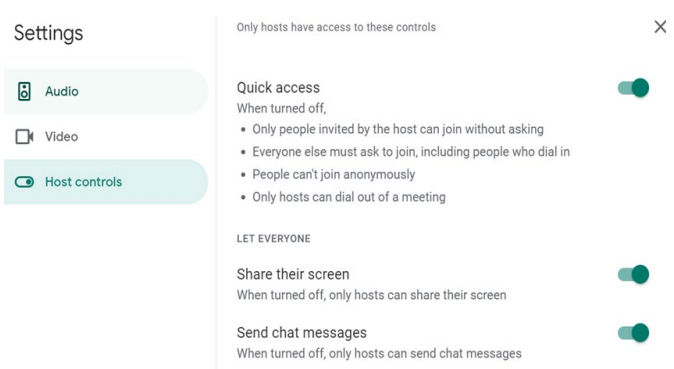
Google Meet and Microsoft teams are the most used tools to deliver live lessons. Here are a few tips in ensuring calls are as secure as possible. Please note, functionality on platforms changes regularly and Microsoft and Google are rolling out updates throughout the Autumn that will impact on how these function.

Google and Teams are designed for communication and collaboration, but at times teachers will want to control when live meets can be joined. We provide remote and in-school training and consultancy for the use of Teams and GSuite for Education, if you would like more information or would like to arrange a session then please get in touch by emailing vikki.bardon@entrust-ed.co.uk

Google Meet Online Safety Tips

Google Meet is a fantastic tool within G Suite for education. The use of Google Meet via a Nicknamed meet, or Google Classroom meet link, will automatically hold students in a lobby until the teacher starts the meeting and the meeting link is deactivated once all participants have left. Once the meeting is ended the students can't restart the meeting if a teacher isn't already in the meeting. Both nicknamed meets and Google Classroom meet links can only be joined by users in your school. Google support Nicknamed Meets

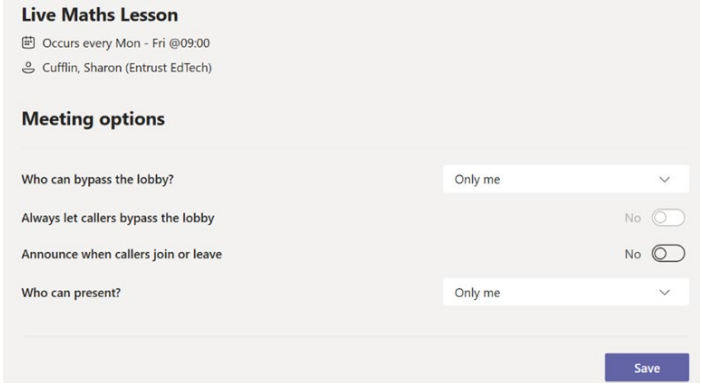
Additional settings can be added to these Meets and can be found in host options, such as everyone must ask to join and only the host can share their screen. The functionality of attendance tracking is coming but only for GSuite Enterprise for Education and not GSuite for Education. Chrome extensions are available for attendance tracking in Google Meet.



Microsoft Teams Live Calls Online Safety Tips

Microsoft allows anyone with the meeting link to join a call. This can be useful if you want a virtual parent meeting without the parent having to log into an account. Teams meetings can be re-joined for 60 days after the meeting has taken place and currently anyone, even students can start the meeting. Microsoft is rolling out student policies that will prevent students from starting a meeting.

Until this policy is in place there are still some settings you can select to safeguard students: Meeting Options can be selected to hold all students in a lobby until a teacher lets them in and permissions on who can present can also be changed. Students will then be admitted to the meeting by the teacher. Attendance lists can be downloaded during a meet showing when attendees joined and left the meeting, very useful for an audit log.



Microsoft is changing where meeting recordings are being saved for more information visit https://docs.microsoft.com/en-gb/MicrosoftTeams/tmr-meeting-recording-change

Safeguarding Considerations when Loaning Equipment to Young People

If you are supplying a device (and connectivity) to a young person or family to support learning at home, then there are a few key points that should be considered to ensure you are doing this in the safest way possible:

- **Acceptable use policy (AUP)** – There should be a specific AUP that spells out the responsibilities of the young person(s) and the parent(s) or carer(s) as to how the device should be used, where the responsibilities lie and what the implications are for inappropriate use.

- **Online safety resources / support** – Parents/Carers should be provided with appropriate resources to ensure they can support their child in using the device in an appropriate way and how they can respond if things go wrong. These should be relevant to your school community and so it may not be appropriate to just provide links to web sites if you know that the family's computer literacy or language skills are not at an appropriate level.

- **Appropriate filtering** – Rather than relying on the parental controls on the home broadband or the very limited mobile filtering provided with a sim card, consider applying filtering to the device so that you have a level of control over what can be accessed whenever the device is connected to the internet. Currently we have seen an increase in access to pornography and other age inappropriate material as well as social media use continuing through most of the night. It is worth noting that this is generally Instagram messages and other chat with no use of Facebook from the young people.

- **Appropriate monitoring** – Digital monitoring software can alert you to potential safeguarding concerns as well as risky or inappropriate behaviour on the device. It is important to understand exactly how the chosen software works and what the limitations are so that you have an appropriate level of cover. Entrust's recommended monitoring software, unlike some of the others, covers what is typed on the device as well as what is displayed on the screen. The latter is particularly important to pick up information that is being sent to the young person through email and chat, for example if they were to receive bullying, threatening or grooming messages.

- **Digital monitoring service** – Reviewing the information generated from monitoring software needs to be carried out regularly by appropriate staff and this takes time. Using a Digital Monitoring Service will ensure that the information is reviewed in a timely manner and any potential issues are escalated to appropriate staff.

- **Device management** – Discuss with your technical support how the device will be kept up to date with any required patches or updates to ensure it is not vulnerable to viruses or malware and how you will control what software / apps are installed on the device.

- **User management** – Will users have their own username or a generic one to access the device. This is particularly important with monitoring software as the information captured will be against the username and machine name. If they are logging on with a generic account such as 'user' or 'student' then you will need to keep a record of which student has which machine name in case you need to follow up on a safeguarding incident.

  While there may be extra time and cost involved in setting this up, we have seen students discussing domestic violence with their friends, searching for information on self-harm and suicide and primary age children with their siblings on Oovoo video chatting with random people.

0333 300 1900 | edtech@entrust-ed.co.uk | www.entrust-ed.co.uk

General Online Safety

Distressing Viral Videos

At the beginning of September, a safeguarding alert was raised by many well-intentioned organisations regarding a viral TikTok video that originated on Facebook Live depicting a man dying by suicide.

We would like to stress the importance in cases like this of not naming specific apps in question or providing too much detail of the footage – which may give rise to more curiosity and sometimes drive more traffic to the distressing footage, but rather provide generic advice about what to do if you see something unpleasant online. Communicate with parents but don't be too specific, just mention that you are aware of a real and particularly nasty viral post going round and share information on how to help their young person (Advice for parents - what to do if your child sees something upsetting online) and for members of staff or individual families who are supporting someone who has seen the video or it has stirred up anxiety or thoughts about suicide Samaritans Internet and Suicide.

Where to go for support...

YoungMinds Crisis Messenger If you are a young person experiencing a mental health crisis, you can text the YoungMinds Crisis Messenger for free, 24/7 support.

YoungMinds Parents Helpline Worried about a child or young person? Contact the Parents Helpline for free, confidential advice via the phone, email or webchat.

Plan your Relationships, Sex and Health Curriculum

The DfE has released its latest guidance to help school leaders plan, develop and implement the new statutory curriculum. The guidance states that teaching should clearly explain the knowledge, facts and concepts needed and provide adequate opportunities for pupils to recall the acquired knowledge, facts and concepts to develop an understanding of the topic.

How up to date is staff knowledge and confidence in delivering the topics of internet safety and harms; online mental wellbeing; online relationships and online and media? We can remotely deliver online safety updates for staff at a time to suit - twilight or staff development day – your staff could be in school or at home and we will live broadcast the content and hold discussions with staff either via Microsoft Teams or Google Meet.

Remote Sessions

We have also turned our Horizon's series of Maintaining Wellbeing in a Digital World into remote sessions for PSHE, Computing and Safeguarding leads to attend and have added another ***new*** session into our Horizon's series which focuses on Live Streaming – the benefits and the risks. There are four webinars in total, each webinar costs £75 to attend:

- **Coping** with the pressures of an online life - delivered by Vikki Bardon – We will discuss potential activities of risk online that can have a negative effect on mental health and begin to understand how using social media and the internet can contribute to changes in a young person's interpersonal behaviour and/or emotional state.

- **An ecological approach** to mental health and behaviour – delivered by a child psychologist - When we can begin to understand how children adapt to their environments in ways that make sense to them, given the psychological and social resources available to them, we have an opportunity to see some of the valid needs behind behaviours. We can also understand why we need to work just as hard at changing the environment children are in as we do in providing individual interventions to improve their mental wellness.

- **SEND** and associated risks with mental health – delivered by a SEND practitioner from a Special School - children with autism or learning difficulties, for example, are significantly more likely to have conditions such as anxiety. Other areas of difficulty include executive functioning skills – the mental processes enabling us to plan, focus attention, remember instructions and juggle multiple tasks successfully; forming trusting relationships; social skills; managing strong feelings e.g. shame, sadness, anxiety and anger; sensory processing difficulties and coping with transitions and change.

- **Live Streaming** – delivered by Vikki Bardon – We will discuss live streaming and understand the merits of why it is popular amongst young people. We will consider the risks and discuss how to mitigate these with appropriate education to address inappropriate online behaviour when live streaming.

Project Evolve Toolkit

If you are not yet aware of or using Project Evolve, then your online safety and relationships, sex and health curriculum could be missing out on some great resources. ProjectEVOLVE is **FREE** to access and sets out to resource each and every one of the statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" outlining the digital knowledge and skills that children and young people should have the opportunity to acquire as they develop. It includes activities, outcomes, supporting resources and professional development materials.

All eight strands have now been fully resourced from Year 1 through to Year 13 of the progressive statements. Use this tool to dip into, to refresh or complement existing resources and lesson activities, discover new ideas which will get your pupils actively involved in learning and understanding about the risks online, recognising the signs, knowing how to help themselves and each other and where to go for support.

Social Media and Algorithms

The word algorithm appears in the Key Stage 1 Computing curriculum and features in the programming elements beyond Key Stage 1. We explain that they are instructions or procedures that allow computers to operate more effectively. However, they also appear in the online world, do you discuss how algorithms are used online and how can they impact children and young people? Algorithms online automatically deliver content to a user based on how they interact and behave online – this explains why you can be looking at a website for a holiday sale and you suddenly see lots of advertisements for holidays and travel on other websites. It's because algorithms use people's history of browsing and interaction with posts to generate 'similar' content, which the algorithm has learnt that you will like.

Link pupils' understanding of algorithms from programming with unintentionally sharing personal data online, and social media addiction to encourage discussion and help pupils see how companies purposely design their services and apps to ensure we remain online for hours at a time. At worst, how it can be problematic when a young person interacts with posts that focus on a certain issue. For example, liking survivor stories of self-harm might result in the young person being bombarded with similar content, which could impact their own mental health, or spreading conspiracy theories about Covid-19. Suddenly they get lots more posts about Covid-19, which may confuse them about what to believe.

Use many of the progressive, age appropriate activities and resources from Project Evolve under the Managing Online Information strand to link all this learning together.

Cyberflashing and 'pile on' harassment targeted in online law reform plans

Law reforms targeting abusive messages, cyberflashing and "pile on" harassment have been proposed in a bid to stem harmful behaviour online. Cyberflashing is when someone sends an unsolicited sexual image to another device nearby and "pile on" harassment is where online harassment is co-ordinated against an individual.

The commission proposes changes to the Malicious Communications Act 1988 and the Communications Act 2003 to criminalise behaviour where a communication would likely cause harm, which would cover electronic attacks such as an abusive email, a social media post, a WhatsApp message or content sent through Bluetooth.

Meanwhile, it is recommended that cyberflashing be included as a sexual offence under Section 66 of the Sexual Offences Act 2003.

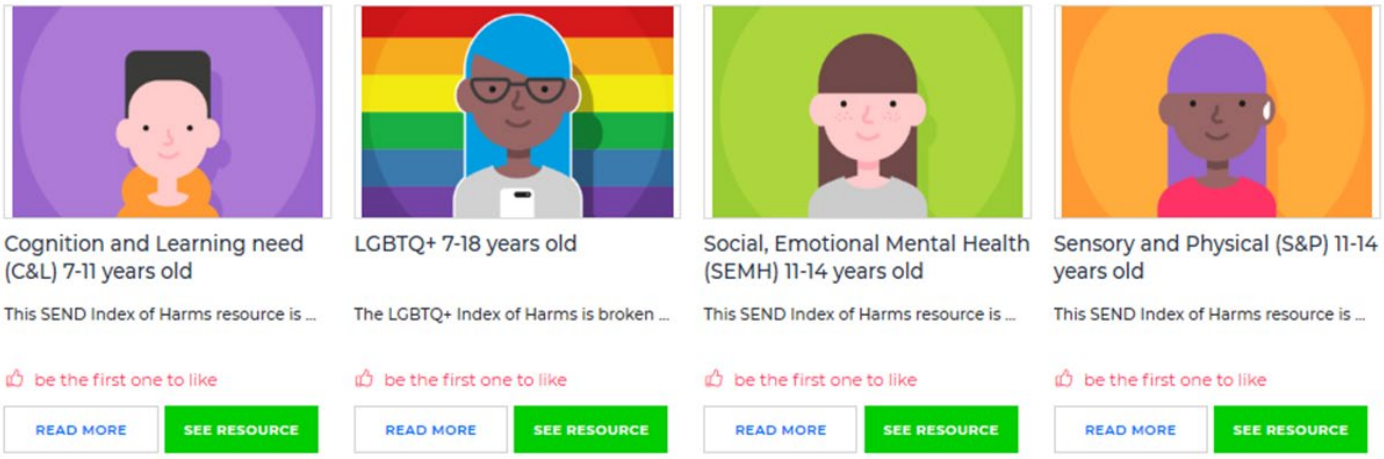
Reforms to tackle the malicious sharing of information known to be false have also been proposed.

0333 300 1900 | edtech@entrust-ed.co.uk | www.entrust-ed.co.uk

New resource - Online Harms Index

This new resource is for professionals and parents of children with vulnerabilities or from minority communities – specifically SEND, LGBTQ+ and children in care. It is being delivered in partnership with Internet Matters and is funded by the Home Office.

This resource links with Education for a Connected World and the Project Evolve Tool Kit. It can be accessed from the Internet Matters website. https://www.internetmatters.org/inclusive-digital-safety/advice-for-professionals/online-harms-index/



360 Degree Safe Online Safety Audit Tool Updated

The 360 tool received significant updates in April 2020. The new tool is easier to use and has many new features. If you have not visited since the update, now would be a good time – so that you can check that your policy and practice continue to meet the updated guidance and benchmark levels.

When logged in, schools will see a radar graph representing their school's position compared to the national level and the benchmark, i.e. aspirational level in every aspect.

The new tool has more data, tools, and reporting features to help you track your progress and plan your improvements. Your levels and commentaries have been transferred to the new tool.

Where aspects have been changed, this data will be transferred from the nearest equivalent judgement to make the process easier for you, which is why it's important to check your levels and commentaries to ensure that your practice still meets statutory guidance.

A recent report from the 360 degree safe Self-Review Data 2020, found that the weakest areas are:

49%
of schools have no governor online safety training. How are they ensuring effective online safety practice?

41%
of schools have no staff online safety training.

Regular online safety training for staff is a statutory requirement and just under half of the schools that use the self-assessment tool are not meeting statutory requirements! Please get in touch to find out about our staff online safety training. We provide sessions specifically for DSLs looking at safeguarding online, for Computing leads looking at the curriculum requirements and for all staff to provide updated guidance and awareness of current issues and trends amongst young people online.

Email vikki.bardon@entrust-ed.co.uk to find out more.

0333 300 1900 | edtech@entrust-ed.co.uk | www.entrust-ed.co.uk

Online Safety Questions for Governors

The UK Council for Internet Safety released a few years ago, 5 key questions for Governors to find out about online safety policy and practice in school. This document has now been completely updated to reflect recent changes in the online safety landscape.

New Parent Guides: Privacy and Personal Information

ThinkUKnow has produced some new guides for parents:

A Parent's Guide to Personal Information
A Parent's Guide to Privacy Settings

Childnet release 25 ideas for embedding online safety throughout the curriculum

Embedding Online Safety - Primary
Embedding Online Safety - Secondary

Short films created by young people to inspire peers to stay safe online and make the most of the Internet

UK Safer Internet Centre has published a blog featuring a series of short films created during lockdown by young people. Use them to inspire your young learners to create their messages for online safety and positive use of the internet.

WhatsApp's Factcheck Feature

Over the summer, WhatsApp added a magnifying glass icon next to messages that have been forwarded through chains of five or more people. Tapping the magnifying glass searches the message's contents online, with the hope that this should reveal if it contains conspiracy theories or misinformation.

Teaching Resources for Fake News and Fact Checking

BBC iReporter - Your role as a BBC journalist is to cover a breaking news story - publishing your story to a "BBC Live" site. Your story will be judged on how well you balance accuracy, impact and speed.

FakeOut - Your social media feed has been infected by false information. Your job is to learn the skills of verification, so you can sort fact from fiction — in the game, and in real life
Horrible Histories Fake News Song

Safer Internet Day – 9 February 2021

The UK Safer internet Centre have announced the theme for this school year which is, 'an internet we trust: exploring reliability in the online world' The internet has an amazing range of information and opportunities online, but how do we separate fact from fiction?

Thinkuknow image sharing resource Send me a pic? *update*

The education resource on consensual and non-consensual nude image sharing among young people contains three session plans based on short film clips. Each clip shows a fictional online chat where young people request, receive and discuss issues related to nude images.The updated resource now includes information about the law on nude image sharing and has been updated on pages 7-8 of the resource pack, with slides 11-13 of CPD presentation for professionals. We've added references to the legislation against non-consensual nude image sharing listed below.

Communications Act 2003, Criminal Justice and Courts Act 2015, Justice Act (Northern Ireland) 2016 and Abusive Behaviour and Sexual Harm Act (Scotland) 2016.

What if my child wants their own YouTube channel?

Where do you start? Is it allowed? Is it a good idea? How old do they have to be? And how do you even do it anyway? Share Parent Zone's article to help parents/carers make a decision.

New toolkit launched to help with FOI compliance

The ICO has launched an online toolkit to help public authorities to respond to freedom of information (FOI) requests. The toolkit is a practical way for public authorities to assess where they are now and what they can do to improve as they return to greater capacity. The first stage of the toolkit focuses on timeliness. Once the toolkit has been completed, a unique report is created. Your report will identify areas of improvement and where action needs to be taken.

Leading Data Protection Webinar

Does the person in your school responsible for leading and helping maintain compliance with data protection laws, require an insight into their roles and responsibilities? We are delivering a webinar to guide them through and remind of their responsibilities on 8 December 9:30 – 14:30 cost £129. To book a place visit https://entrust.education/Event/115995

Entrust Virtual Online Safety Conference 2021

This year we will be hosting our annual Online Safety Conference virtually! We would love as many of you to join us as possible. Don't miss out on what is set to be an informative webinar, providing an opportunity to gain information that can support your school and improve your own knowledge and awareness in current online safety matters.

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 delivering sessions during the webinar.

All we can say for the moment is hold the date Wednesday 27 January 2021. More details will follow regarding speaker line up and times for the webinar.

Finally...

Congratulations to Emily Rogers from Etching Hill CE Primary Academy, Rugeley who has successfully gained the personal accreditation for EPICT Online Safety through attending the EPICT Fast Track course and completing the assessment!

We are here to help!

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

vikki.bardon@entrust-ed.co.uk
M: 07805 692 102
sharon.cufflin@entrust-ed.co.uk
M: 07885 236 140