School Improvement
Liverpool

June & July 2020
paul.bradshaw@si.liverpool.gov.uk
@silesafety

Online Safety Update

FAO Headteachers, Designated Safeguarding Leads
& Computing Subject Leaders

Welcome to issue 29 of the Online Safety Update brought to you by School Improvement Liverpool.

This half-termly 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.

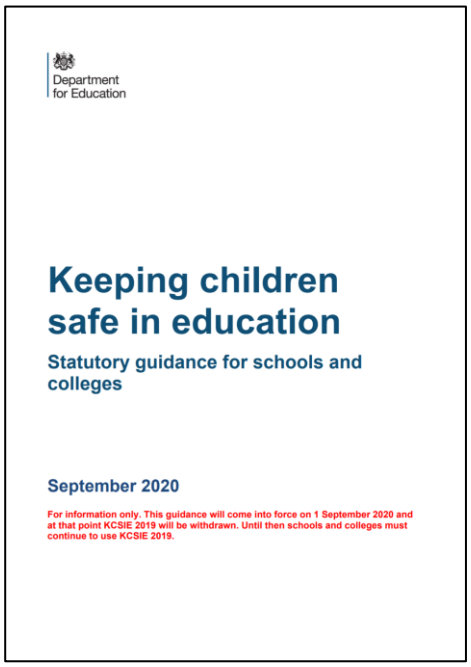
If you would like to access the resources/documents referenced in this update, you can locate them by visiting this link: http://bit.ly/silonlinesafetyupdates

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

Keeping Children Safe in Education (effective 01/09/20)

KCSIE is statutory guidance from the DfE, which all schools and colleges must have regard to when carrying out their duties to safeguard and promote the welfare of children.

The expanding role of technology to facilitate learning in a way many educational settings have not previously explored as a result of the Covid-19 pandemic means online safety should be a key consideration for all educational settings. As the online safety agenda continues to evolve and increase; it is vital that Headteachers, DSLs and governing bodies are able to evidence that they recognise the importance of online safety within their statutory safeguarding responsibilities for all members of their community.


Department for Education

Keeping children safe in education

Statutory guidance for schools and colleges

September 2020

For information only. This guidance will come into force on 1 September 2020 and at that point KCSIE 2019 will be withdrawn. Until then schools and colleges must continue to use KCSIE 2019.

The London Grid for Learning, LGfL (of which Liverpool City Council is a partner organisation) has produced a helpful tracked change document comparing KCSIE 2019 and KCSIE 2020, respectively, with substantive changes highlighted in yellow.

https://safeblog.lgfl.net/?post=1205

Credit is also due to Rebecca Avery from Kent County Council/The Education People who has identified the key online safety foci from the "new" KCSIE – see below.

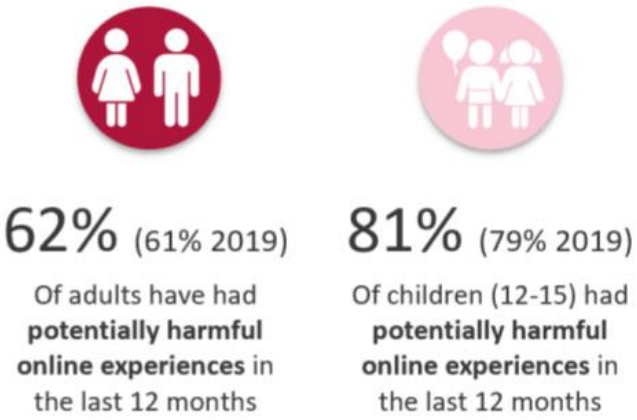
Summary of key online safety requirements and changes within KCSIE 2020

- DSLs continue to have overall responsibility for online safety (Annex B) and this cannot be delegated. They can be supported by appropriately trained deputies and liaise with other staff on matters of online safety.
- DSLs should continue to be able to evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff should continue to be provided with online safety training at induction and as part of regular child protection training and updates.
- Part five continues to recognise that child on child sexual violence and sexual harassment can occur on and offline.
- Additions have been made to content relating to Child Sexual Exploitation and Child Criminal Exploitation to recognise the role technology can play.
- An additional section has been added to part one to help staff make the link between mental health concerns and safeguarding issues. Whilst online safety is not specifically addressed, the section signposts to guidance and resources where online safety is explored.
- Links to additional and updated resources have been included to support schools and colleges in teaching online safety to all learners as part of a broad and balanced curriculum.
- Additional information within Annex C is available on how to support the safety of children online, while they are learning at home in response to the Covid-19 pandemic.
- Content relating to 'Upskirting' has been updated to reflect that anyone of any gender, can be a victim.
- Additional links to new guidance and resources related to online safety have been added throughout the document and in particular in Annex C.

https://www.theeducationpeople.org/blog/online-safety-and-keeping-children-safe-in-education-2020-summary-document-for-designated-safeguarding-leads-and-senior-leaders/

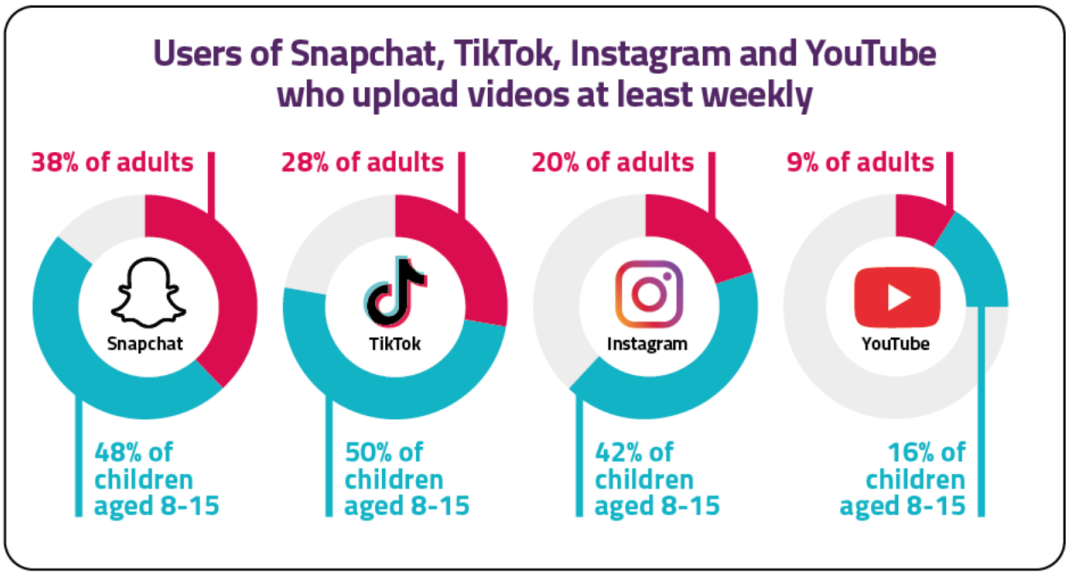
For your added convenience, I have appended **KCSIE Annex C: Online Safety** to the end of this Update

Ofcom Online Nation 2020 report (published 24/06/20)



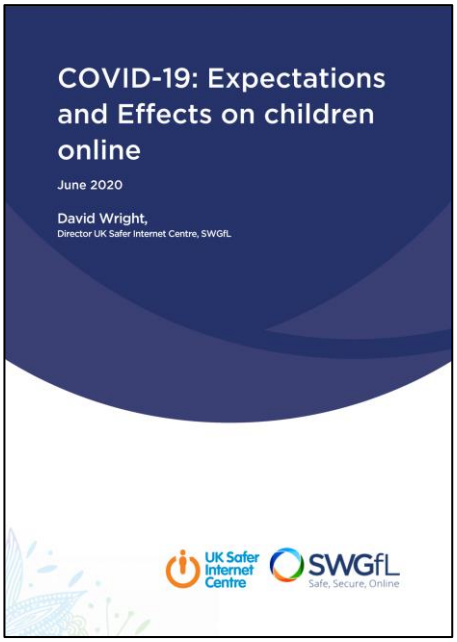
Definitely worth a read. Download it from the link at the beginning of this Update or from the Ofcom website - https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/online-nation

People remain wary about online safety with 87% of adults saying that they had concerns over children using video-sharing websites and other apps.



Ofcom's director of strategy and research Yih-Choung-The states, "Lockdown may leave a lasting digital legacy. Coronavirus has radically changed the way we live, work and communicate online, with millions of people using online video services for the first time."

The COVID-19 Digital Effect



Covid-19 has affected the lives of billions of people across the world, with unprecedented peacetime restrictions imposed. The reaction has been an extraordinary digital migration; a migration online to maintain some form of normality in terms of social, economic, entertainment and learning.

In this resource, David Wright (Director of UK Safer Internet Centre) looks at the expectations and effects COVID-19 has had towards children online.

https://swgfl.org.uk/assets/documents/covid-19-expectations-and-effects-on-children-online.pdf

In terms of the early evidence published, this would suggest that

- Whilst many children have access to technology and connectivity, this is not universal and the 'digital divide' will have an impact

- In terms of child sexual abuse content online, there has been an increase of individuals searching for child sexual abuse content, alongside an increase in access to adult content online.

- Children have reported heighted anxiety associated with the pandemic and restrictions

- Parents are anxious that their children's education will be impacted

Just 19 pages – worth a read!

Keep it real online

This is a great new free resource produced by the New Zealand government for parents and carers. It features four videos which are worth a watch.

Find out more about the campaign here - https://www.keepitrealonline.govt.nz/

I have populated the QR code at the front of this Update with the four NZ videos available, together with an online safety video from yesteryear, the classic - **"Where's Klaus?"**, that you may wish to share with parents.

Better Internet for Kids

On 23 June 2020 the International Telecommunication Union (ITU) launched its new **2020 Guidelines on Child Online Protection (COP)**, a set of recommendations for children, parents, educators, industry and policy makers on how to contribute to the development of a safe and empowering online environment for children and young people.

The guidelines for children are available in a child-friendly format and they consist of three resources: a story book for children under 9, a workbook for children aged 9 to 12, and a social media campaign and microsite for children and young people aged 12 to 18.

The guidelines for parents and educators offer guidance to parents and educators supporting children and young people's online lives. They aim to raise awareness of the potential online threats younger users can be vulnerable to, while at the same time encouraging adults to ensure their children have access to high quality, stimulating digital experiences.

https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=6191364

Send me a pic?

THINKUKNOW's new educational resource SendMeAPic is for children aged 12-14 on nude image sharing. The resource has been mapped to the curriculum and contains three sessions, with supporting worksheets and videos.

Whilst SendMeAPic may seem more relevant to older children, younger pupils need reminding not to get undressed or changed online, too – London Grid for Learning have produced a song, animation and activity pack at undressed.lgfl.net - great to get this message across for younger kids.

In response to requests from schools, LGfL have also created a parent letter template you can use or adapt to send to parents, outlining **key principles to support children online**, including friendship and bullying, sharing scary things and getting undressed. Read / download the letter in word format from SafeBlog here.

Cyber Choices – Merseyside Police

https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices

Detective Sergeant John Black from Merseyside Police has been in touch to flag “Cyber Choices”. DS Black currently works in the Cyber Dependant Crime Unit. As part of his role, he looks after Cyber Prevent which comes under “Cyber Choices”.

“Cyber Choices” exists to ensure that the Government’s National Cyber Prevent Strategy is represented across each Region and into local police forces.

The main aims of “Cyber Choices” are to deter people (including young people) from getting involved in Cyber Crime and to prevent re-offending for those who have been involved with cybercrime.

‘Cyberland’ is an online resource where children and young people aged 12-18 can get involved in protecting the virtual city, ‘Cyberland’ from a cyber-attack.

Within ‘Cyberland’ there are 16 interactive exercises which include the fundamentals of cyber security such as firewall configuration and a module on the **Computer Misuse Act (1990)**. Young people can also explore career opportunities linked to their digital skills -see https://cybergamesuk.com/ for more details.

Access is free until September 2020 to help mitigate the potential increased risks of young people becoming involved in cybercrime over the summer, either knowingly or by mistake.

You may also want to share this website with your parents –

https://parentinfo.org/article/help-your-child-make-positive-cyber-choices

And finally, I have also attached an article from the latest issue of the free “**Hello World”** magazine entitled **“Safeguarding in online lessons”** that you may find useful.

https://helloworld.raspberrypi.org/

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 C: Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

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

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 93-95. Resources that could support schools and colleges include:

- Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- PSHE association provides guidance to schools on developing their PSHE curriculum
- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements

This document is for information only and does not come into force until 1 September 2020. Schools and colleges must continue to have regard to KCSIE 2019 until then.

- Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources
- UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Protecting children

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.

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 consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

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.[119] 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.

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

---

[119] The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions

This document is for information only and does not come into force until 1 September 2020. Schools and colleges must continue to have regard to KCSIE 2019 until then.

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCIS has published Online safety in schools and colleges: Questions for the governing board to help responsible bodies assure themselves that their online safety arraignments are effective.

Education at home

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges-and-other-providers and safeguarding-and-remote-education

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 89) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 93), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

This document is for information only and does not come into force until 1 September 2020. Schools and colleges must continue to have regard to KCSIE 2019 until then.

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 sexting-in-schools-and-colleges and using-external-visitors-to-support-online-safety-education

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

This document is for information only and does not come into force until 1 September 2020. Schools and colleges must continue to have regard to KCSIE 2019 until then.

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
- Lucy Faithfull Foundation StopItNow resource 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

[Please edit the following text / delete as appropriate. Feel free to paste into your school letterhead / add your logo and share with parents in any way.]

June 2020

Dear parents,

Staying safe and being a good friend on apps, sites and games

Children and young people have spent much more time on devices than ever before during lockdown, so as we approach the summer holidays, here is some information about staying safe online and principles you can help us remind your children about.

There is a handy fridge flyer to help parents at toptipscorona.lgfl.net which you may want to print out and keep.

Please do not worry too much about screen time - think instead about screen quality, balance and mental health. The Children's Commissioner has provided a framework called the 'Digital Five a Day' with five things to think about each day to help put that into practice.

It is really important children get the opportunity to chat to friends, so it's great to hear that many of them have been chatting online during lockdown. We are sure that this will continue over the summer, so please help us reinforce some key messages about appropriate behaviour to keep everyone safe and happy.

[edit as appropriate whether your school / local area or not]

There have been reports of children being upset by bullying on chat apps, as well as some very distressing images being shared between friendship groups. This can usually be avoided if we remind children and young people to look out for their friends, not say anything that they wouldn't like to hear themselves, and always stop or stand up for others if someone gets upset.

Please remind your children never to share scary or rude images, even to complain about them. If they do see something that worries them or that might be wrong, all they need to do is ask for help from a trusted adult. They could talk to you or to us, or they may feel more comfortable talking anonymously to Childline. If you or they are concerned about an adult's behaviour towards a child online, report them to CEOP. And as a parent, you can also contact the NSPCC - O2 advice line on 0808 800 5002.

One more thing - this may sound like more relevant to older children, but the very youngest children need reminding not to get undressed or changed online. There's a fun song to get this message across at undressed.lgfl.net (plus background information for you).

Thank you for your support - do let us know if you have any questions.

Yours,

SAFEGUARDING IN ONLINE LESSONS

How do you organise live learning sessions that are both safe and help young people to learn? **Carrie Anne Philbin** investigates

Transitioning learning from a face-to-face interaction to online can sound straightforward, especially as we now live in a society where it's common to have access to devices and the internet. In a school environment, it is easier to promote the welfare of young people and vulnerable adults and to keep them safe, thanks to well-established routines built on decades of learning. So in this new world we find ourselves in, how do we promote the well-being of young people while they learn with you online? Here are some tips that might help, based on feedback and ideas from brilliant educators, and leading children's charities such as the NSPCC (nspcc.org.uk), who have tested different approaches to hosting online sessions.

There are four areas to think about if you want to host online teaching sessions:

- Choosing the right technology
- Communicating with young people and parents
- Designing your session
- Child protection

Choosing the right technology

There are lots of different tools that you could use to host live sessions, and they vary in their functionality, cost, and usability. When choosing a technology, think about how you intend to use it and how your intended audience will use it. Consider whether it allows private communication between you and young people, or between young people, as this could be a safeguarding risk. Use your school account and not a personal account when using online tools, and check the privacy settings. It's also a good idea to test the functionality of the technology with colleagues, perhaps by having a practice run of your session. They can stress-test any interactive features, and provide you with useful feedback to incorporate before you run it with students.

Another consideration is access. Does the technology you want to use require young people to have an online account? This may be an issue for learners below the age of 13. Do check your school e-safety policy, as it is likely that there is already guidance available on this issue.

SAFEGUARDING ONLINE GUIDES FOR TEACHERS

- NSPCC Undertaking remote teaching safely (**helloworld.cc/NSPCC**)
- GOV.UK Education for a Connected World Framework (**helloworld.cc/govuk**)
- UK Government Coronavirus safeguarding guidance (due to be updated in June) (**helloworld.cc/safeguarding**)
- Childnet-Teachers and Professionals Section (**helloworld.cc/childnet**)
- UK Safer Internet Centre-Social Media Guides (**helloworld.cc/guides**)

Communicating with young people and parents

Every organisation that provides activities for children and young people needs to get consent from parents or carers for their child to participate. A well-written consent form will support your efforts to ensure parents, carers, and children understand the benefits and risks of online lessons, as well as providing written consent for children to take part. The NSPCC have an example consent form to help get you started (**helloworld.cc/consent**).

It's also a good idea to share a link to your online session in advance with parents, carers, and young people, as well as any instructions they will need for joining. You could also share what you are planning for your learners to work on, including links to any online projects or PDF files they may need. This will help your students to prepare for the session, and keep their adults informed about the learning you want them to experience.

Designing your session

Like any lesson, you should design the session structure and prepare your materials before you announce that you're going live online. If it is the first time using the online technology, I'd recommend having an introduction or starter activity that gives students the opportunity to play with the features. If there is a live comment stream, you might ask them to all say who they are and what they're hoping to learn in the session. I find that allowing this type of structured play reduces the opportunity for misusing the technology later.

You can share instructions in advance

> WHETHER TEACHING ONLINE OR IN CLASS, YOU HAVE THE SAME SAFEGUARDING RESPONSIBILITIES AS A TEACHER

You should consider where you are going to present your session from. The NSPCC suggests you should be in 'a neutral area where nothing personal or inappropriate can be seen or heard in the background'.

I'd also advocate having another teacher or responsible adult acting as a teaching assistant during the lesson. They can moderate any feature misuse and keep an eye out for any safeguarding issues.

Child protection

Whether you are teaching online or in class, you have the same responsibilities as a teacher, and that means if you see or hear anything that worries you during the session, or a child discloses anything to you via email, then you must disclose this to your child protection lead immediately. Make sure you have their contact details to hand and check your school's safeguarding and child protection policy and procedures. (HW)

CARRIE ANNE PHILBIN

Carrie Anne is Director of Educator Support, Raspberry Pi Foundation, and host of Crash Course Computer Science and GeekGurlDiaries, leading educational resources for the NCCE.