NetSupport

Online Safety Guide

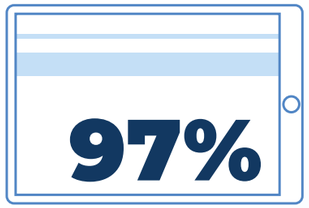
2024

Contents

What is online safety?

Such is the fast-paced nature of the internet; the rewards and the risks are always changing. It is a great place full of wonder and opportunities for fun and collaboration but, as with any activity, risks can arise. The difference is of course with the internet, these risks come in the form of online issues – online abuse, grooming, bullying, sexting, harassment or exposure to inappropriate content such as that of a violent or sexual nature.

With AI now being a far more developed technology, online safety and digital literacy for students and adults takes on new importance, especially in light of the opportunities it creates for bad actors to engage with young people through chatbots, sophisticated fake news campaigns and many more approaches, particularly those that generate Child Sexual Abuse Material (CSAM).



of 3 to 17-year-olds went online in 2022

Source: Ofcom

Working together to protect young people

Much like a lighthouse safeguards ships from rocky shores, our role is to shine a light on safe online practices. We guide young people through the digital world with straightforward tools and clear strategies, helping them navigate safely.

Recognising that technology use doesn't stop at the end of school, society must do what it can to work together to protect young people from potential online harm. This is why in this year's Keeping Children Safe in Education (KCSIE) update there is an added expectation that school governors hold online safety as a central theme in their whole-setting approach to safeguarding and must complete relevant training as part of their induction. In addition, there is an increased focus on recognising and understanding the impact of domestic abuse on children, including its potential short-term and long-term detrimental effects on their health, well-being and learning ability.

What is this guide?

This guide aims to offer approaches and resources to help schools, children and families make the most of the online world, whilst giving advice and support on how to safely navigate a space which, whilst wonderful, can have so many pitfalls.

Cyberbullying

What is cyberbullying?

Defined as repeated behaviour which is intended to hurt someone either physically or emotionally, bullying can happen in real and virtual spaces. It often involves targeting people because of their race, gender, religion, sexual orientation or other aspect, such as their appearance or due to a disability. It can take a variety of forms, such as social bullying, cyberbullying, name-calling, sexual bullying or general threatening behaviour.

With more and more data being gathered by online platforms such as social media sites, knowledge of gender, race, age and interests can help sophisticated software to create chatbots that emulate humans to engage young people in increasingly complex ways.

Online disinhibition can often exaggerate actions and words online and, in recent years, we have seen increasing incidents of cyberbullying taking place on online forums such as:

- texting services and iMessage
- chat platforms such as Messenger, Snapchat, and WhatsApp
- online platforms such as Reddit and Discord
- social media sites such as Instagram, Facebook and Twitter
- online gaming platforms.

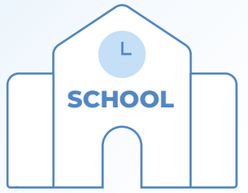
What to be aware of?

Many platforms can facilitate cyberbullying and it is easy for children to access them. The internet never stops, and issues can be difficult to pin down as they often happen over time and are emotional rather than physical. The impact that cyberbullying brings can be significant, with victims being more than twice as likely to self-harm or attempt suicide.

What can you do?

Children see parents/guardians and teachers as being their two main sources for information[1], so aim to create a culture with young people where they can talk to you. Whether you are a parent/guardian or a teacher, ensuring you are approachable and that you make it clear that it is okay to talk will go a long way to help protect a child.

Learn more: [1] SWGfL, Internet Matters, National Bullying Helpline, NSPCC



Nearly 72%

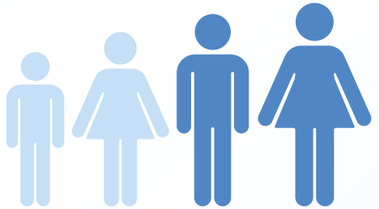
of UK children who had experienced cyberbullying experienced it at school or during school time. [3]

32%

of US 9-12-year-olds say cyberbullying affected their friendships. [1]

26%

of UK children did not report their cyberbullying experiences to anyone. [3]



Between the ages of

10 and 18

the risk of being cyberbullied increases by 2% each year. [2]

Sources: [1] Cartoon Network report, [2] Security.org report, [3] ONS

Fake news

What is fake news?

Fake news is false or misleading information presented as legitimate facts in the style of a news report. It ignores the principles of journalism that ensure that information is accurate and credible. Instead, it is designed to manipulate readers' interpretations of real events, to cause disruption or division.

We are all presented with news on our devices, 24/7. Even the UK Prime Minister has been found to have shared inaccurate information from his personal X/Twitter account. Given this, and the fact that those in politics can spend tens of thousands of pounds per day on social media advertising, how can we identify what is real and what isn't? It's just as easy for adults to be caught out by fake news as it is for young people, so we all need to confirm that what we are reading is a true representation of the facts.

How can we check?

When reading news, be on the lookout for:

- misleading headlines written as clickbait
- propaganda
- poor quality writing
- spoof or parody reporting.

Then, there are things you can check to ensure you're not potentially being misled.

- Be alert and adopt a critical mindset when reading news.
- Check the author – are they known and credible?
- Check the story – has it been published anywhere else?
- Check the source – being well-known can be helpful but doesn't always indicate that the truth will be told. There's a big difference between reading news from established providers or social media posts.
- Check that images are original – Google Lens includes a reverse image search.

You can even verify facts for yourself on established sites such as FactCheck, Snopes or BBC Verify.

'Inaccurate news'

Another angle to consider is that the internet is full of articles and blogs that are based on fact but may not be accurate. These are not published to intentionally mislead people, but most self-publishing writers may not apply all the necessary checks and standards that qualified journalists do, so you may still need to verify any facts before sharing or quoting a post.

'Sponsored news'

Finally, news and reviews are often shared because they are a form of propaganda, shared by media outlets and/or influencers on their social media channels to promote a product, brand or ideology. Things to look for are small icons that say 'Ad' or things such as #Sponsored in the text comments. Often, however, despite there being guidance for influencer marketing from the Advertising Standards Authority (ASA), many are not transparent about their sponsored posts and articles. It is down to us to be savvy to know when we are being sold to.

Almost

60%

of 12-15 year olds in the UK use social media as a news source.

12-year-olds

are more likely to tell a teacher about seeing fake news but 15-year-olds are more inclined to ignore it.

41%

of 12-15 year olds believed they had seen deliberately misleading news on social media.

Source: Statista, Microsoft, BBC

Gaming

What's the problem?

Play is an important part of learning and of growing up. Playing games digitally brings additional opportunities for learning and growth – and not just from those that promote problem-solving, maths practice or fine motor control and hand-eye coordination.

When it comes to gaming, the problem often isn't with young people having too much fun, although screen time can be an issue. Many games that young people want to play are what are known as Massively Multiplayer Online Role-Playing Games (MMORPGs). These types of games involve players playing together online in the same space, communicating through headsets or by typing messages.

These games are great fun for young people and gained huge popularity during the pandemic when they were starved of their ability to play together in real life. The social interaction however can bring issues that will concern parents and guardians, such as:

- **Addiction.** When excessive online gaming starts to affect areas of a young person's life, such as schoolwork, sleep or appearance, it's time to act. As with any addiction, withdrawal can be difficult, so managing time spent online before it gets to that stage is wise.
- **Cyberbullying.** The social side of gaming has grown, and it is now possible to interact with players all over the world. However, as ill-intentioned people may hide behind online personas, parents can help protect children by checking device settings, keeping gaming consoles in shared areas, and playing games together.
- **Screen time.** Young people need guidance and support to regulate their screen time, whether they are playing games, investigating the internet or watching YouTube videos. House rules such as keeping devices out of bedrooms, using parental controls, and parents setting an example by modelling device-free time are recommended.

Sources: Internet Matters, NSPCC

57% of UK children aged 3-15 play games online. [3]

76% of US children under 18 play video games. [1]

12-17 year olds were most likely to play against people they didn't know. [2]

Roblox is the most popular games app among UK children **aged 8-12.** [3]

Sources: [1]Cloudwards, [2]Ofcom 2022 report, [3]Ofcom 2023 report

Grooming

What is grooming?

At its simplest, grooming involves a person gaining another's trust so they can later abuse it – or even them.

Young people are especially vulnerable to grooming. After all, it's flattering when someone takes a special interest, whether it's a stranger or a person who they already know. Grooming can lead to Child Sexual Exploitation (CSE), trafficking, involvement in county lines and more, so it's vital to be alert to the signs.

Groomers infiltrate a young person's online world by inhabiting the same spaces as they do. This can be on social media, messaging apps, gaming forums or even plain old email. Young people are often unaware that they are being groomed. Sometimes it's adults doing the grooming – but not always.

AI chatbots

What is even more startling is that there are now AI chatbots that can do this automatically, without bad actors needing to do much of the grooming themselves. If you are keen to see an AI chatbot in action so you can see how sophisticated it can be, Snapchat has an integrated chatbot called 'My AI' (although you can give it whatever name you want). In a world where a bad actor could have many chatbots grooming on their behalf, where they can continue a conversation once it has hooked in an unsuspecting victim, we need to be even more aware of this increasingly concerning area.

What are the signs?

Parents are often unaware that their child is being groomed until the process is well under way. However, there are some changes that they can watch out for, such as their child:

- having new items in their room not bought by parents or carers
- being secretive and not talking about how they spend their time at home or at school
- suddenly having money from an unexplained source
- going missing from home and/or not explaining where they've been when they return
- being withdrawn or upset
- not going online or to activities they have previously enjoyed
- having an older boyfriend/girlfriend
- missing school or activities
- using alcohol or drugs.

Where to turn to for help

If you find CSE images online, you can report it to the Internet Watch Foundation.

The NSPCC's 'Report Remove' allows young people to report images or videos shared online and see if it is possible to get them taken down.

Report online grooming in Canada via the national tip line at cybertip.ca or get support in the USA at RAINN.org.

In the UK, online grooming crimes recorded by police increased by around

70%

in the three years up to 2021. [1]

56% of parents think children are most at risk of being targeted through social media. [2]

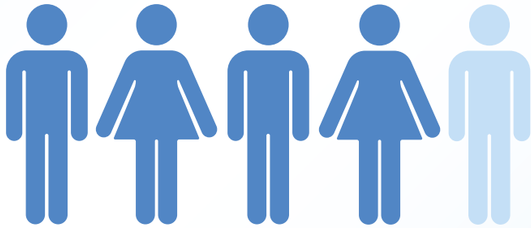
In 2021, Instagram was the most common site for grooming and was recorded by police in

32%

of instances where the platform was known. [1]

4 in 5

parents are worried about children being groomed online for criminal exploitation. [2]



30%

of 12-15-year-olds said they had been contacted online by a stranger wanting to befriend them. [3]

Sources: [1] NSPCC, [2] The Children's Society, [3] Internet Matters

Radicalisation

What is radicalisation?

Radicalisation is the process a person goes through as they adopt extreme beliefs about race, religion, politics or gender. Those who are radicalised often end up being drawn into hate crimes, violence or terrorism, joining extremist groups and alienating themselves from family and friends.

The internet is perfect for those seeking to radicalise and draw others to their cause because of the sheer number of communication channels available. Mainstream social media apps may often be the trigger for young people to further investigate views they are exposed to, especially if they are posted by popular influencers or are 'celebrities' in their field.

Bad actors can, as with grooming, use sophisticated techniques such as AI-generated chatbots or social media campaigns which draw in impressionable young people.

Signs to look out for

Being a part of a group appeals to all of us, young people included, but those who are vulnerable are at increased risk. Changes in behaviour are often the first indicator that something is going on, such as:

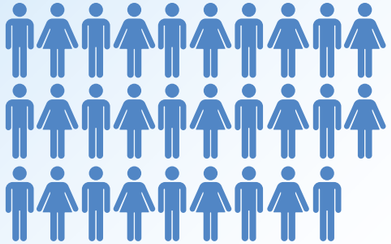
- no longer considering others' points of view
- changing/falling out with friends
- being argumentative
- being sympathetic to conspiracy theories
- being secretive
- having new online friends they don't talk about
- having multiple online identities
- reading extremist content online.

Keep an eye on social media

Radicalisation takes time. Watch out for increased use of less mainstream social media platforms such as Discord, BIGO LIVE, Yee, Hoop and more. Young people are often unaware that they are being radicalised, as their 'friends' take their time to gain their trust.

The UK Prevent Duty sets out requirements for schools to follow to protect students from radicalisation. and parents to reach out to for this and other issues.

Useful information



In the UK, police arrested

29 teenagers

for suspected terrorist-related activities between March 2021 and March 2022. [1]

US organisation, RAND, interviewed former extremists, who said that mental health, marginalization and propaganda played a part in their radicalization. [2]

The Action Counters Terrorism website has practical help for parents who are worried their children may be being radicalised.

Europol's Internet Referral Unit, scans the web for online terrorist material and refers it to host platforms. It has assessed more than

42,066

pieces of content to internet companies since 2015. [3]

Sources: [1] Counter Terrorism Policing, [2] RAND, [3] EU Parliament

Sexting

What is sexting?

Sexting usually involves someone sending nude or semi-nude photos and explicit videos of themselves to another person, who may then share them with others or post them online without consent. The person who is the subject of the photo or video has no control over who it is being sent to, potentially leaving them feeling humiliated and susceptible to bullying and extortion.

In addition to the emotional effects, the content will have a lasting 'digital footprint' which can be hard to remove, only adding to its long-term impact on the person involved.

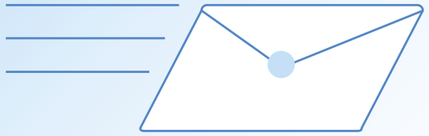
What you should know

1. In many countries, it is illegal to send/receive underage sexual content. In around half of US states it is illegal for under-18s to sext, on child pornography (child sexual abuse) grounds.
2. In the UK, it is an offence to make, distribute, possess or show any indecent images of anyone aged under 18, even if the content was created with the consent of that young person. [1]
3. Sexting is increasingly common amongst children who have vulnerabilities and often occurs due to pressure or extortion.

Where to find help

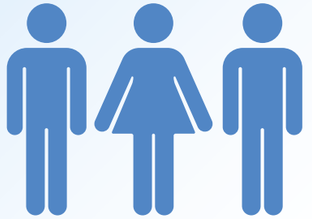
- The NSPCC's 'Report Remove' allows young people to report image or videos shared online and see if it is possible to get them taken down.
- The UK government has published advice for schools on dealing with sexting.
- CEOP (run by the UK National Crime Agency) has an online safety centre for children and parents to reach out to for this and other issues.
- The CyberBullying Research Center publishes what each US state's sexting laws cover.
- Take It Down is a US organization that helps with removal or stopping the sharing of nudes.

Source: [1] Child Law Advice



Nearly 40%

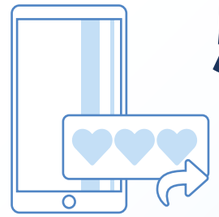
of all teenagers have posted or sent sexually suggestive messages. [1]



X100

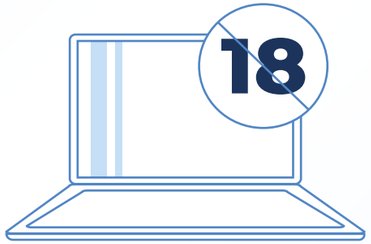
In the UK during 2019, more than 300 children of primary school age were investigated for sexting offences. [3]

17% of sexters share the messages they receive with others, and



55%

of those share them with more than one person. [1]



Platforms like OnlyFans and Omegle likely contribute to the spread of self-generated sexual imagery as neither have robust age verification checks in place. [2]

Sources: [1] DoSomething.org, [2] Internet Matters, [3] The Guardian

AI-generated Child Sexual Abuse Material (CSAM)

What is CSAM?

"Child sexual abuse material is a result of children being groomed, coerced, and exploited by their abusers, and is a form of child sexual abuse. But using the term 'child pornography' implies it is a sub-category of legally acceptable pornography, rather than a form of child abuse and a crime." – NSPCC, Jan 2023

"Child Sexual Abuse Material (CSAM) has different legal definitions in different countries. The minimum defines CSAM as imagery or videos which show a person who is a child and engaged in or is depicted as being engaged in explicit sexual activity." – INHOPE, 2021.

What is CSAM?

There are an increasing number of cases where faces cloned from real photos of young people can be placed onto AI-generated bodies – and these can be programmed to emulate scenarios classed as CSAM. So, without any real CSAM activity taking place, the photo of any child can be used to generate this kind of content. Cases such as this one in Spain are becoming increasingly common: "AI-generated naked child images shock Spanish town of Almendralejo" – BBC News, September 2023

What can we do about it?

- Regularly update your knowledge about the latest technologies and methods used in creating AI-generated CSAM. Awareness is key to prevention, so staying informed about the evolving nature of these threats can help in identifying and reporting them effectively.
- Teach young people about the risks of sharing personal images online. Emphasise the importance of digital privacy and the potential misuse of their photos in the creation of AI-generated CSAM.

- For schools and educational institutions, it's vital to have strong online safety policies that include specific guidelines on AI-generated materials. Regularly review and update these policies to reflect new threats and technologies.

Friend of NetSupport, ESafety Adviser, Alan Mackenzie, has shared this AI-generated CSAM advice video (only suitable for adults). He advocates using the Report/Remove tool created by the IWF in partnership with NSPCC, which is suitable for secondary and college students.

The IWF reported that

20,254

AI-generated images were posted to one dark web CSAM forum in a one-month period.

Source: IWF

Social Media

Social media is a complex subject for teachers, students and parents. Children often feel compelled to be on it and are drawn in with infinite scrolling and constant notifications. Teachers often must deal with the repercussions of things that happen there. Parents don't know what to do and are often pressured by their children to let them use it, even when they are under the recommended age.

Bad actors (people who deliberately or carelessly harm others) share content on these platforms – just think of Andrew Tate and his misogynistic posts. Content from these bad actors interacts with platform algorithms that personalise and amplify it to who they think is the best audience.

Social media is big business. In 2021, 44% of all global spending on advertising was with Meta (Facebook/Instagram) and Alphabet (Google) owned businesses. Facebook, Instagram and YouTube are machines that aim to maximise engagement time on the platform to sell more advertising. Couple this with research from the Children's

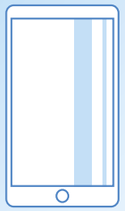
Commissioner for England that reported that one in five boys watches porn at least every day and that more than half of frequent users seek out violent sex acts, there's lots to consider about what we allow our children to access.

People often assume that the age 13 rating on social media apps comes from a place where children are emotionally mature enough to use them. This is not the case. The rating comes from the legacy setting of the USA's COPPA (Children's Online Privacy Protection Act, 1998) legislation which made it illegal to collect or store the personal information of children under age 13. According to Ofcom's Online Nation 2023 report, the majority of children in the UK use WhatsApp by the time they are 10 years old.

What to be aware of

- Algorithms on social media aren't written with children in mind. They're created to keep people on the platform, collect their data and promote advertising to them.
- Social media sites can be addictive using likes, notifications, followers, colour schemes, infinite scrolling and other features to help keep people engaged.
- Social media platforms promote the sharing and creation of content and can facilitate cruel and bullying behaviour, such as trolling and cyberbullying.
- Social media is often a misrepresentation of real life, where a world of influencers and celebrities sharing content can exert unnecessary pressure to fit into an unattainable mould.
- It can cause feelings of anxiety, depression and loneliness. If posts don't receive engagement or likes, it can cause significant upset to children who perceive it as being personal.
- When talking with young people about posting online, share the THINK acrostic which asks: Is it TRUE, is it HELPFUL, is it INSPIRING, is it NECESSARY, is it KIND?

Be informed! WhatsApp is a 16+ app despite it showing on the App Store as a 12+ app and on the Play Store as being appropriate for everyone. UKSIC (UK Safer Internet Centre) says "We recommend following WhatsApp's guidelines."



A 2019 survey

found that Instagram affected the way US and UK teens feel about themselves and their mental health, with 12-23% saying it made them feel 'somewhat worse' and 2-3% saying 'much worse'.

63%

of 8-11 year olds use social media apps or sites.

12-15-year-olds

spent more time online or on social media (1hr 24 minutes) per day than they did being with friends.

Just under two-fifths

of 3-4-year-olds (38%) have their own profile on YouTube.

Source: Ofcom

How can schools help tackle these issues?

The four key strands a school can use to help mitigate these online safety issues are:

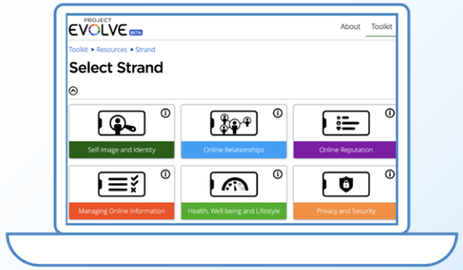
Educating children about the risks

In England, Ofsted, Keeping Children Safe in Education and the National Curriculum for Computing require education settings to deliver online safety education through their broad and balanced curriculum, from the youngest phases right through the key stages. It is also a statutory requirement for teachers to receive training. This isn't a statutory duty internationally, but it is widely regarded to be an essential part of all school curricula. The UK Government's recently updated "Meeting Digital and Technology Standards in Schools and Colleges" is also very clear about the importance of online safety as a thread that runs throughout the various sections.

Resources to support learning

Many organisations, such as the UK Council for Internet Safety (which created the framework of 'Education for a Connected World') and others (e.g., Google's 'Be Internet Awesome' curriculum) have created fantastic resources for supporting learning about how to help keep yourself safe online.

One particularly useful resource for schools is the brilliant Project EVOLVE tool, brought to you by the SWGfL (South West Grid for Learning), Nominet and the UK Safer Internet Centre. Whilst UK curriculum-centric, its free resources are superb and aligned across the main areas schools everywhere should be considering teaching to young people.



If you're in the US, ISTE has a great curriculum within its ISTE Standards for Students which covers digital footprint, online behaviour, intellectual property and data privacy. The curriculum goes beyond this within the other strands to help embed responsible uses of technology to support and transform learning; they are well worth a look.

There are also products you can use as a school to help support online safety in your curriculum, like the award-winning Natterhub, which also has support options and curriculum information for parents. With a library of more than 350 lessons, it covers the primary curriculum requirements with teacher-led and independent animated lessons for you to use with your classes.

Awareness days

Celebrating relevant awareness days in your school, such as the annual Safer Internet Day, Digital Citizenship Week or Mental Health Awareness Week are a great way to draw spotlights onto the importance of online safety but it's important to try and remember that every day should be a Safer Internet Day.

Educating staff about the risks

Safeguarding is everyone's responsibility in education, whether you are teaching or support staff. There are several ways schools can educate all staff about the risks, but a key feature of any strategy is to ensure that it does not happen in silos.

Planned staff training (CPD/Inset)

Scheduled and planned safeguarding training is a statutory requirement for all staff so that colleagues are well equipped to identify, support and help young people who need it, when they need it.

Staff training should also inform colleagues of the latest updates to legislation or best-practice advice such as KCSIE, Children's Internet Protection Act (CIPA), DfE or other bodies that provide guidance around online safety support.

The bigger picture

Scheduled and planned safeguarding training is a statutory requirement for all staff so that colleagues are well equipped to identify, support and help young people who need it, when they need it.

Undertaking ongoing reviews of where the school organisation sits against a clear framework – such as that provided by the Online Safety Review tool from SWGfL – is a great way to both benchmark your provision and highlight areas for improvement.

Interweaving online safety into the fabric of your day-to-day curriculum is where best practice sits. Educating staff about the resources available, how to support young people and how to role model best practice themselves, all help to provide the best support possible.

The theme of Safer Internet Day 2024 is "Inspiring change? Making a difference, managing influence and navigating change online". To help you do this, check out NetSupport's CPD resources. You might also like to consider looking at our Head of Education, Mark Anderson's ICT Evangelist resource called 'IDEAL' – a framework for positive digital citizenship and digital literacy.

Effective monitoring tools

Schools in England have statutory duties surrounding online safety, device monitoring, filtering and data privacy. There are several tools you can use to help monitor and control what students are doing online, both in supervised and unsupervised environments, including KCSIE and CIPA. But to fulfil their duties, schools need to do more than just internet monitoring through a firewall.

There are compelling educational reasons for not blanket banning everything. For example, we wouldn't want to stop children learning about areas like online safety, where difficult results and topics such as sexting and pornography might come up. We do, however, want children to not have access to tools and sites that share and promote this content.

Just as blanket blocking and internet monitoring do not provide context, a lack of tracking means you're missing crucial information when understanding students' issues and the reasons for seeking out this content in the first place.

Learn how NetSupport's solutions can help address these issues and what your duties are.

Seek the bigger picture

Considering solutions that allow for contextual analysis as part of your internet monitoring processes could be a better approach. Tools such as NetSupport DNA or classroom.cloud are prime examples that do this brilliantly (and have won awards too!).

Contextual analysis is useful when tracking what young people are typing because it helps to provide insight into their thoughts and feelings. It helps to identify any potential risks or concerns, such as signs of cyberbullying or self-harm. It can also provide an understanding of the context of messages, helping to identify any potential red flags and allowing adults with safeguarding responsibility to intervene and provide support in the moment before a situation escalates.

The algorithms in NetSupport's tools use variables to consider surrounding activities, such as search parameters used, the time of day and websites being visited (including previous activities that have triggered alerts). All of these help to create a 'risk index'. This index ultimately helps adults to identify genuine concerns and balance them according to the risks shown.

Time and time again, schools have contacted us to tell us how these tools have helped highlight problems bubbling beneath the surface that, if hadn't been caught, would have most likely led to much more concerning issues.

Working with parents/carers to support young people

The key to success here as a school community is to involve parents and carers in what you are doing in school to support their children around all aspects of school life, not just online safety. Here are some ways you might like to consider working with parents/carers to support young people.

Invite parents to digital parenting events

Holding regular events for parents to attend to learn about different strategies or tools to support their children are often very well received and a great tool in providing a wrapper of care. Topics often include gaming, online harm prevention, screen time, use of devices, parental controls and many more.

Use digital signage

By sharing important messages on digital signage in high traffic areas that parents visit, they will soon see that online safety is high on your school's agenda.

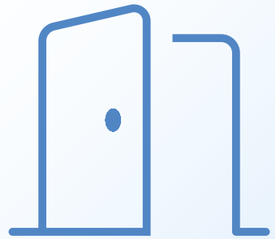
Survey parents and students

As seen from the research shared by the i-vengers organisation, perception and reality of what parents think is happening with their children are often at odds with each other. By comparing the results of like-for-like surveys of both parents and learners, you will uncover some great talking and learning points about where young people may need additional support.

Some actions for parents

- **Discuss online safety with your children**

Some research shows that talking about these issues with your children will help them to feel proud of you, as their parent, for wanting to have honest conversations about how you want to help and support them online. By choosing safe boundaries together you help foster a positive conversation around safe and responsible use of technology and online spaces.



- **Open door policy**

It's difficult to always keep an eye on your children, but by having a simple 'door open' policy when gaming at home can be a great start. Being aware of sites such as the Family Gaming Database is useful to know exactly what games are about and their capabilities.

- **Communication with the school**

Hopefully, as a result of the school having open channels of communication and regular touchpoints for conversations around online safety and curriculum, parents will feel confident to report to the school if they have any concerns around online safety that their child or other children might be facing. The school can then act upon any information to help, in ways such as monitoring during school hours or with learning opportunities within the curriculum.

Summary

Whichever way you look at it, we all have a responsibility to be mindful about online safety and ensure children are properly safeguarded. The sections within this guide should inform your thinking and your provision, but it should not *be* your provision.

Please refer to our useful resources and tap into the opportunities that they provide.

You can also stay updated about any new resources we create on our NetSupport social media feeds:

Twitter/X Instagram LinkedIn

Useful resources

Glossary

Term	Definition
AI-generated CSAM	Child sexual abuse imagery generated by artificial intelligence
County lines	Refers to gangs who extend their drug dealing business into new locations outside their home areas and almost always involves exploitation of vulnerable young people.
CPD	Continuing Professional Development. Also referred to as Professional Development.
CSAM	Imagery of videos which show a person who is a child and engaged in or is depicted as being engaged in explicit sexual activity
CSE	Child Sexual Exploitation.
Cyberbullying	The act of bullying through online channels such as apps, games and forums.
DSL /School Counselor	Member of staff in a school with responsibility for online safety/safeguarding.
Fake news	Untrue or deliberately misleading information presented in the style of a news report.
Filtering and monitoring	The practice of schools having appropriate technology measures in place to monitor students' online activities and restrict their view of inappropriate material.
Firewall	A technology security measure to monitor incoming and outgoing network traffic based on a set of security rules to keep organisations' technology safe.
Grooming	To build a relationship, often with a young vulnerable child, with a hidden objective of sexual abuse or engaging them in criminal activity.
MMORPG	Massively Multi-player Online Role Playing Game.
Online abuse	Any type of abuse that happens online.
Online disinhibition	The loss of inhibitions that can stem from not speaking to people directly whilst using online platforms.
Online safety	Being aware of and taking measures to mitigate the possible risks that may occur on the internet. In schools, this combines digital citizenship teaching with EdTech solutions to help children learn to keep themselves safe online. An alternative term for 'safeguarding.'
Radicalisation	A process by which an individual or group comes to adopt increasingly extreme political, social or religious ideals and aspirations.

Safeguarding	Being aware of and taking measures to mitigate the possible risks that may occur on the internet. In schools, this combines digital citizenship teaching with EdTech solutions to help children learn to keep themselves safe online. An alternative term for 'online safety.'
Trafficking	A process where young people are forced or persuaded to leave home for the purpose of exploiting them.
Trolling	Trolling is the act of sharing hate or negativity about a person online that causes upset
Sexting	Sending sexually explicit messages, photos or videos via a digital device.

Events

Digital Citizenship Week
Held annually during the third week of October.

Mental Health Awareness Week
13th-19th May 2024

Safer Internet Day
6th February 2024

Official guidance

Children's Internet Protection Act
CIPA - USA

Children's Online Privacy Protection Rule
COPPA - USA

Keeping Children Safe in Education
KCISE - UK

UK Prevent Duty

Resources and solutions

Solution/Resource	Description
classroom.cloud	Three-in-one solution for online classroom instruction, online safety and IT management.
Family Gaming Database	A family gaming database of educational online games
Google Lens	Google's search engine for images.
iVengers	Peer-led digital leader programme to engage, educate and empower young people to make safer choices online.
National Online Safety	Online safety education for educators, parents and children.
Natterhub	EdTech solution for online safety in primary schools that prepares pupils to thrive online.
NetSupport DNA	EdTech solution for IT Management and Safeguarding in education settings.
Persona Life Skills	Online social-emotional learning for teenagers.

References

BBC Newsround (2019), *Fake news: What is it? And how to spot it*. Available at: https://www.bbc.co.uk/newsround/38906931 (Accessed 1 February 2024)

Cartoon Network (2020), *Tween Cyberbullying in 2020*. Available at: https://i.cartoonnetwork.com/stop-bullying/pdfs/CN_Stop_Bullying_Cyber_Bullying_Report_9.30.20.pdf (Accessed 1 February 2024)

Child Law Advice (2022), Sexting. Available at: https://childlawadvice.org.uk/information-pages/sexting/ (Accessed 1 February 2024)

Childline, *Online grooming*. Available at: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/ (Accessed 1 February 2024)

Cloudwards (2022), *23 Video Game and Online Gaming Statistics, Facts & Trends for 2023*. Available at: https://www.cloudwards.net/online-gaming-statistics/ (Accessed 1 February 2024)

Counter Terrorism Policing (2022), *Upward trend in children arrested for terrorism offences*. Available at: https://www.counterterrorism.police.uk/upward-trend-in-children-arrested-for-terrorism-offences/ (Accessed 1 February 2024)

DoSomething.org, *11 facts about sexting*. Available at: https://www.dosomething.org/us/facts/11-facts-about-sexting (Accessed 1 February 2024)

Educate Against Hate, *Signs of radicalisation*. Available at: https://educateagainsthate.com/signs-of-radicalisation/ (Accessed 1 February 2024)

European Parliament (2021), *Radicalisation in the EU: what is it? How can it be prevented?* Available at: https://www.europarl.europa.eu/news/en/headlines/security/20210121STO96105/radicalisation-in-the-eu-what-is-it-how-can-it-be-prevented (Accessed 1 February 2024)

Internet Matters, *Online gaming – The risks*. Available at: https://www.internetmatters.org/resources/online-gaming-advice/online-gaming-the-risks/ (Accessed 1 February 2024)

Internet Watch Foundation, How AI is being abused to create child sexual abuse imagery. Available at https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/ (Accessed 1 February 2024)

Learn about online grooming. Available at: https://www.internetmatters.org/issues/online-grooming/learn-about-it/#online-grooming-facts (Accessed 1 February 2024)

Learn about sexting. Available at: https://www.internetmatters.org/issues/sexting/learn-about-sexting/#sexting-facts (Accessed 1 February 2024)

Microsoft 365 Life Hacks (2022), *How to Spot Fake News*. Available at: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-to-spot-fake-news (Accessed 1 February 2024)

National Literacy Trust (2018), *Fake news and critical literacy: final report*. Available at: https://literacytrust.org.uk/research-services/research-reports/fake-news-and-critical-literacy-final-report/ (Accessed 1 February 2024)

NSPCC, *Online games*. Available at: https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-games/ (Accessed 1 February 2024)

Grooming. Available at: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/ (Accessed 1 February 2024)

Record high number of recorded grooming crimes lead to calls for stronger online safety legislation. Available at: https://www.nspcc.org.uk/about-us/news-opinion/2021/online-grooming-record-high/ (Accessed 1 February 2024)

Ofcom (2021), *Children and parents media use and attitudes report 2020-21*. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf (Accessed 1 February 2024)

Ofcom, Children and Parents: Media Use and Attitudes 2023. Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0027/255852/childrens-media-use-and-attitudes-report-2023.pdf (Accessed 1 February 2024)

Office for National Statistics (ONS) (2020), *Online bullying in England and Wales: year ending March 2020*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/onlinebullyinginenglandandwales/yearendingmarch2020 (Accessed 1 February 2024)

RAND Corporation (2021), *What Do Former Extremists and Their Families Say About Radicalization and Deradicalization in America?* Available at: https://www.rand.org/pubs/research_briefs/RBA1071-1.html (Accessed 10 January 2023)

Security.org (2022), *Cyberbullying: Twenty Crucial Statistics for 2023*. Available at: https://www.security.org/resources/cyberbullying-facts-statistics/ (Accessed 1 February 2024)

Statista (2019), *Instagram and its effects on mental health according to teens in the United States and United Kingdom in 2019*. Available at: https://www.statista.com/statistics/1280619/us-uk-teens-instagram-effects-on-mental-health/ (Accessed 1 February 2024)

The Children's Society, *Keeping children safe online*. Available at: https://www.childrenssociety.org.uk/what-we-do/our-work/preventing-child-sexual-exploitation/online-safety (Accessed 1 February 2024)

The Guardian (2019), *Thousands of children under 14 have been investigated by police for sexting*. Available at: https://www.theguardian.com/society/2019/dec/30/thousands-of-children-under-14-have-been-investigated-by-police-for-sexting (Accessed 1 February 2024)

NetSupport

Online Safety Guide

2024

www.netsupportdna.com
classroom.cloud