

NetSupport



Online Safety Guide

2022

Contents

What is online safety?	3
Grooming	4
Cyberbullying	6
Sexting	8
Concerning games/challenges	10
Radicalisation	11
Social media	13
How can schools help tackle these issues?	15
Educating children about the risks	15
Educating staff about the risks	16
Effective monitoring tools	17
Actions for parents	19
Summary	20
Glossary	20

What is online safety?

With technology and the internet being part of everyday life (and especially since 2020 with remote learning in place across the world), online safety is key – and by that we mean keeping safe online.

“Our members are only seeing age-appropriate content on the internet.”

– Explore Learning

A young person’s online world may consist of social media, chat forums, online games, websites and more, all of which can be accessed via laptops, mobile phones and tablets. This makes them incredibly accessible, 24/7, and opens them up to new online risks, from grooming, cyberbullying and radicalisation, to sexting and more – meaning that it’s more important than ever to educate young people about these threats, how to be a good digital citizen and how to keep themselves safe online.

Learn more ➔

in the official guidance (England): KCSIE paragraphs 31-52

Schools and parents working together

The internet is ever present, so that means online safety issues do not simply start and stop at the school gate or within the home; the risks extend across both locations and beyond. Therefore, to successfully protect students from online dangers, a joined-up approach with schools and parents/carers working together is best.

Legal requirements

Most countries have guidance and requirements in place for schools to implement tools and online procedures to keep students safe, while also teaching them about online safety, in and outside of school. For example, you can find more information from the **UK Government here** and for the **USA, here**.

“The Online Safety features provide alerts when students are interacting with potentially harmful materials online. Previously this information had to be cobbled together from multiple sources or was simply unavailable.”

– Hillcrest Academy

Let’s explore the topics...

Grooming

What is grooming?

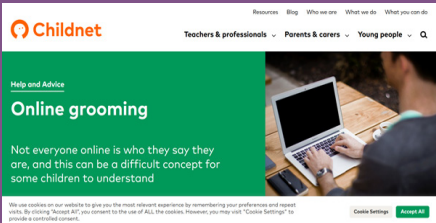
Grooming is commonly explained as the process that takes place when someone builds a relationship, trust and emotional connection with a child or young person so that they can manipulate, exploit and/or abuse them in some way (for instance, by sending naked photos, sexual images or even meeting up in person).

Anybody can be a groomer (a known person or stranger), no matter their age, gender or race. Often, it's an adult pretending to be a young person – but not always. Sadly, grooming often takes place on the same sites, games and apps that young people use to socialise and collaborate.

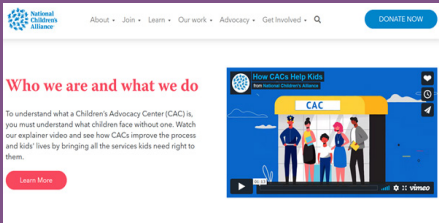
What to be aware of:

- A child is unlikely to know they've been/are being groomed.
- It's very difficult to spot, as there are often no obvious signs.
- The groomer may be building up trust over months and years.
- Live streaming is becoming more prevalent with the content being captured and distributed widely across other sites.

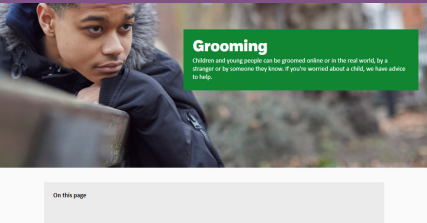
Useful resources



Childnet International -
Online Grooming



National Children's Alliance



NSPCC - Grooming



44%

of the webpages actioned by the Internet Watch Foundation in 2020 contained self-generated imagery.

More than 70%

of grooming instances were found on these apps (during 2018-19, where UK police recorded and provided the communication method):



1 IN 5

grooming victims in the UK (in 2019) were aged 11 or younger.



In 2018, a Spanish study found online grooming can significantly impact the mental health of the victim associated with:



Cyberbullying

What is bullying?

Bullying is usually defined as hostile behaviour that is unsolicited. It involves an imbalance of power between the bully and the victim, whether it is real or not. It's a behaviour that is often repeated with the intention to harm or control. There are various types of bullying (physical, social and verbal) and it can include threatening behaviour, physical or verbal attacks, isolating the victim from friends and other students, starting and spreading rumours and more.

In recent years, bullying has moved to the internet (cyberbullying) and is prevalent on:

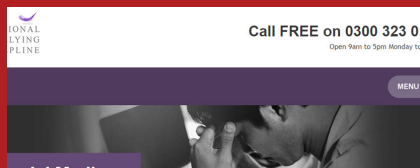
- Social media, such as Facebook, Instagram, Snapchat and Tik Tok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging and online chatting over the internet
- Online forums, chat rooms and message boards, such as Reddit
- Online gaming communities

What to be aware of:

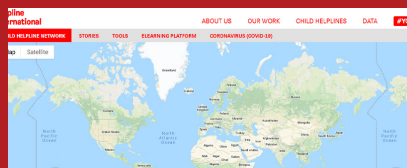
- **Persistent** – The internet doesn't stop and so neither does cyberbullying. It's very difficult to escape from, as there are many platforms that facilitate it.
- **Permanent** – Digital content is very hard or near impossible to delete, especially if the posts get shared, so it stays visible to peers and strangers in your digital footprint.
- **Hard to notice** – Cyberbullying is emotional over physical and, with so many platforms where it can happen, it's very hard for parents and schools to know what is going on.
- **Wellbeing** – Students who are bullied report being unable to focus, physical ailments, mental health impacts such as anxiety and depression, as well as low self-esteem.

Learn more  more in the official guidance (England): KCSIE paragraphs 13 and 28

Useful resources



National Bullying Helpline



Child Helpline International



Unicef



34% of students

in the US have experienced cyberbullying at least once.

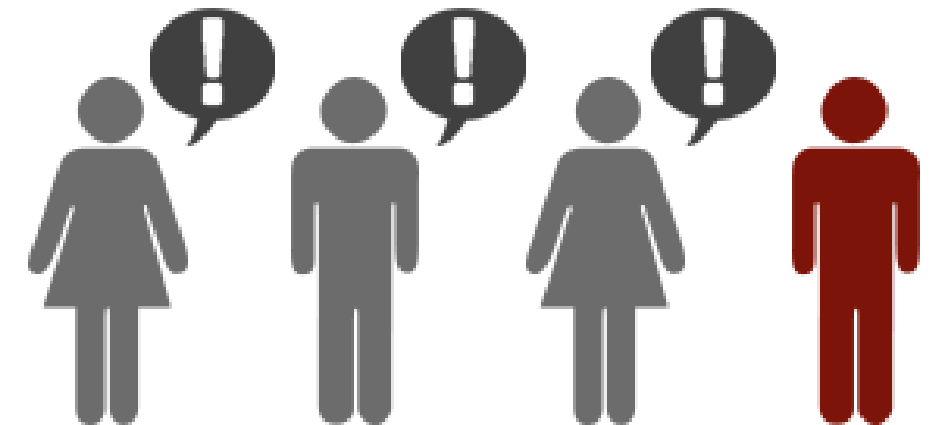
64%
(2 in 3)

of students in Canada feel that bullying is normal and a routine occurrence in their classrooms.



26%
(1 in 4)

of UK 10-15 year-olds did not report being bullied online to anyone.



Information sources: [TechJury](https://www.techjury.co.uk/) | [bullying.co.uk](https://www.bullying.co.uk/) | [Our Family World](https://www.ourfamilyworld.org/)

Sexting

What is sexting?

Sexting is sending sexually explicit messages, photos or videos via a digital device. It often also involves people sending nude or semi-nude photos and explicit videos of themselves. People of any age group can sext but it is more common among teens.

What to be aware of:

- Sexting increases with children who have vulnerabilities (such as hearing loss and speech difficulty) and is likely to have occurred due to pressure or blackmail.
- Once sent, the person has no control over how and where images and messages might be shared online by other people. It can leave them vulnerable to bullying, humiliation and embarrassment, or even to blackmail.
- The consequences of sexting can quickly spiral out of control, with some images even going viral.
- 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.
- In many countries/states, it is illegal to send/receive underaged sexual content (i.e., in the US, in about half of states it is illegal for under-18s to sext – on child pornography (child sexual abuse) grounds).

Learn more  in the official guidance (England): KCSIE paragraph 49

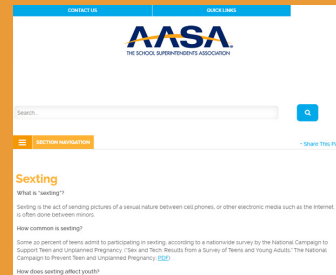
Useful resources



Internet Matters -
Look At Me



Online Safety
Commissioner



AASA

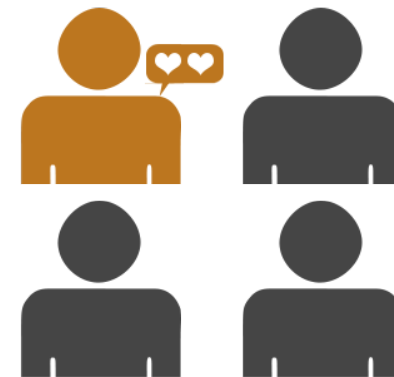


GOV.UK

A recent global study
found that of

110,000
teens

(under 18)
around the world,



1 in 4

have received sexts
(sending and receiving
sexts were 14.8% and 27.4%
respectively).

The study found that

12%

had forwarded a sext without
asking consent and



8.4%

had had a sext forwarded
without their consent.

Information sources: [Internet Matters](#) | [Nationwide Children's](#) | [Teaching Times](#) | [NSPCC](#)

Concerning games/challenges

What are these?

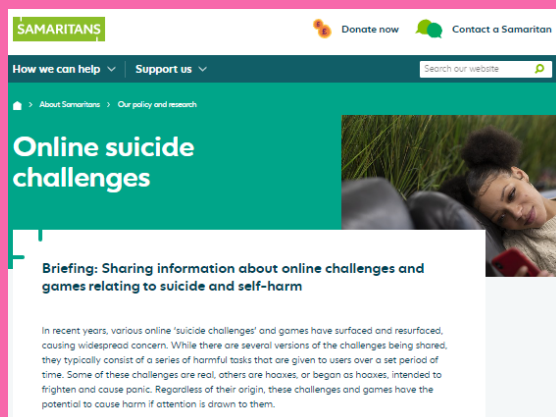
They range from games that encourage self-harm (such as the Salt and Ice challenge, Neknomination and Cinnamon Challenge) or, more seriously, 'suicide games' which involve a series of challenges, ending in suicide (Blue Whale Challenge, Momo and the Fire Fairy). It is important to note that many of the 'suicide games' have been reported as hoaxes and there is little or no evidence to suggest that they have been linked to any suicides. Many of these games are created with the sole purpose of going viral to boost an online profile page.

With this in mind, a cautious approach is needed when highlighting any trending games, as sharing or recirculating these can simply scare and misinform if not supported by a credible source.

What to be aware of:

- The games/challenges tend to surface on social media and chat forums.
- New games/challenges are constantly being created, meaning it's very hard to keep up to date with the latest trends – and whether they are a real concern or another hoax.
- Real or not, it could lead to some children playing them and causing self-harm accidentally.

Useful resources



[Samaritans.org - Online suicide challenges](https://www.samaritans.org/online-suicide-challenges)

Information sources: [Samaritans](https://www.samaritans.org/online-suicide-challenges)

Radicalisation

What is radicalisation?

Radicalisation is the process through which a person comes to support or be involved in extremist ideologies, usually focused on politics, religion, gender and/or race. The person is encouraged to adopt beliefs or are persuaded to join groups whose views and actions are generally considered extreme. It can result in a person becoming drawn into terrorism and hate crimes.

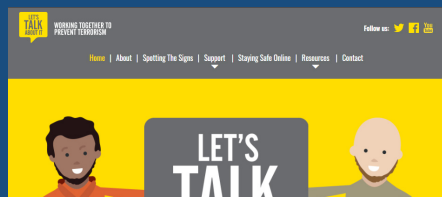
Through the internet, children may be exposed to these views and receive information that can begin their interest.

What to be aware of:

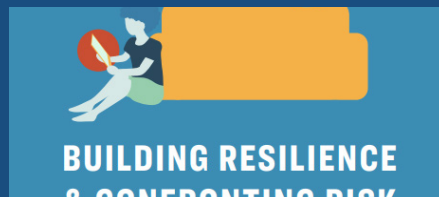
- Anyone can be radicalised, but children are more susceptible to it simply because they can be impressionable and easily influenced. Being a part of a radical group can offer a sense of belonging or purpose, which can be especially appealing to vulnerable children and teenagers who are figuring out who they are.
- It's a gradual process that takes months or years and often the interaction moves to less mainstream social media sites, such as Kik Messenger, Whisper, Yik Yak or Omegle. Often, the child is unaware that their beliefs are being reshaped, as groomers build up trust over a significant period of time.
- There are specific policies and requirements for schools to follow to protect students from radicalisation, such as the **UK Prevent Duty**.

Learn more  in the official guidance (England): KCSIE page 30

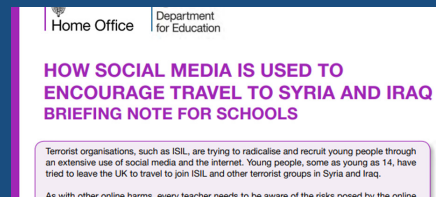
Useful resources



[Let's talk about it](#)



[Southern Poverty Law Center](#)

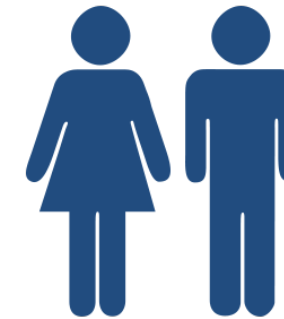


[Department for Education](#)

During 2019-20
the UK education
sector made

1071

referrals to the
government
anti-terror
scheme.

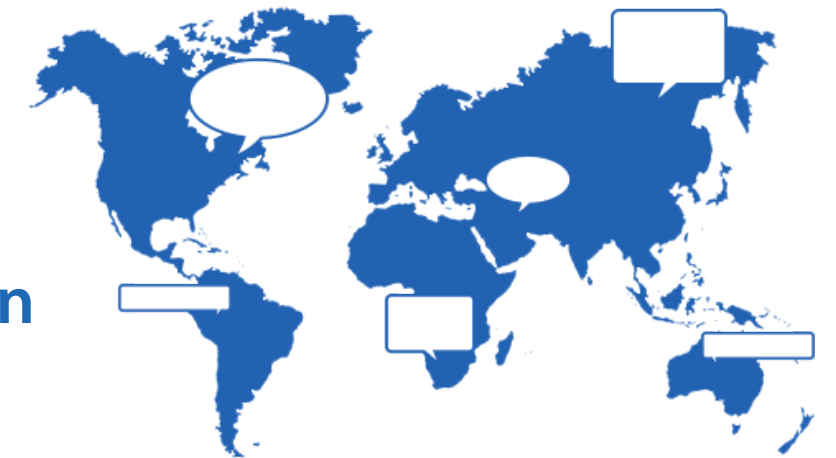


Terrorist organisations in many
places all over the world consider
school environments



as attractive recruitment places.*2

Extremist groups, especially
ISIS, benefit from the use of
the internet and social media
as they enable cheap
mass communication
across borders.



Information sources: [Internet Matters](#) | [Department for Education](#)

Social media

What is social media?

Social media is a collective term for platforms and apps where people can share digital content or participate in social networking.

Social media is often used by people to connect with friends and family, but with the rise of mobile social media applications such as Facebook, Twitter and Instagram, it has become more accessible to younger children, who have embedded it into their everyday lives.

Nearly all social media services have a minimum age restriction of 13 years old, yet **Ofcom** found that underage social media accounts were on the rise with over half of 11 and 12-year-olds having them.

What to be aware of:

- **Appears addictive** - Social media is built around likes, views, followers, infinite posts, notifications and messages, making it appear highly addictive/compelling for some young people.
- **Facilitates cruel behaviour** - Social media can be a great way for children to communicate with each other. However, it can also be a platform for more negative behaviour, such as cyberbullying and 'trolling', because communication is indirect and so it's easier to make cruel comments.
- **Depression and anxiety** – Social media can be a misrepresentation of reality. Many social users will post content that makes them look good or seem interesting or that may encourage lots of engagement (likes etc.). Since peer acceptance is crucial for children, others seeing those posts may feel compelled to promote an equally perfect life. They perhaps will reflect on the realities of their own life, which seems inferior in comparison, and feel that they are somehow missing out (FOMO).
- **Loneliness** - Although social media enables everyone to be hyperconnected, it can cause loneliness. In addition, young people may feel hurt and ignored should their posts not receive immediate engagement.
- **Negative influence** – Social media is full of filtered and edited images, influencers, models and celebrities, all adding to the pressure that young people feel to try to achieve an impossible body image which can, in turn, sometimes lead to eating disorders. Unfortunately, the internet is awash with websites that help sufferers to conceal their disorder and promote how to lose weight in unhealthy ways - so education is key.



A study found that British 14-24 year-olds agreed that their
wellbeing is being damaged by social media

with platforms such as



Snapchat was cited in particular for making young people feel negative - creating feelings of worry from being left out.

Learn more



in the official guidance (England): KCSIE paragraph 37; page 24, 31 and 37

A 2019 study of more than
6,500
12 to 15-year-olds
in the US found that those who spent
more than

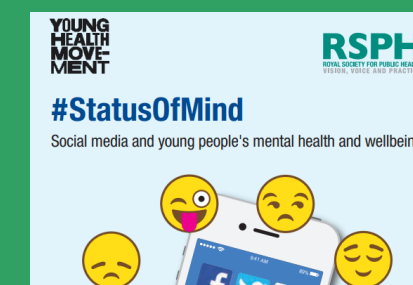


using social media were at a higher risk of experiencing depressive symptoms.*¹

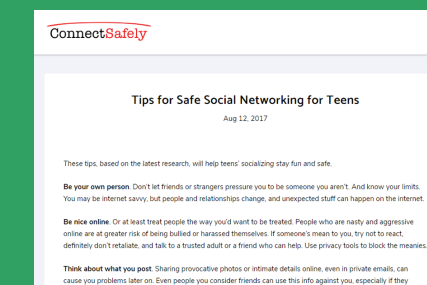
Useful resources



Internet Matters



RSPH - Status of mind



Connect Safely

Information sources: [Child Mind Institute](#) | [Wiley Online Library](#)

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.**

**Educating
staff about
the risks.**

**Employing
effective
monitoring
tools.**

**Actions
for
parents.**

Educating children about the risks

Digital citizenship

This all begins with education, from both a technological and a social and cultural perspective. Often, this broader topic is referred to as digital citizenship. There is no shortcut to discussing openly (and, ideally, regularly) the best ways to stay safe online and to make children aware of the risks that can and do exist. Teaching children best practice on the use of social media (not sharing personal information, long-term risks and implications of sharing inappropriate photos, appropriate language, the ever-present risk of grooming and so on) has never been more important in the current climate.

Spreading awareness of the dangers of social media can help prevent young people from being dragged into unsafe situations. To help, parents can:

- Make sure children are aware that social media isn't an accurate representation of reality (nobody posts about their low points).
- Minimise screen time and encourage hobbies and activities.

"When teaching online safety, the risks often outweigh the opportunities. Technology isn't going away, it's embedded into life; embrace it and if you want impact, balance the positives and inject the risks. Don't teach by fear."
– Alan Mackenzie, Online Safety Specialist

Peer-led education

Student engagement is key and so creating an environment that encourages student voice or allows for student digital leaders (cyber clubs and digital newsletters that students can be encouraged to help author) can be a great starting point to gaining their involvement and opening up a dialogue between them and school leaders.

Awareness days

Celebrating awareness days in the school and creating activities around them can really help to raise awareness of a particular topic, e.g., Safer Internet Day, Mental Health Awareness Week and so on.



Safer
Internet
Day

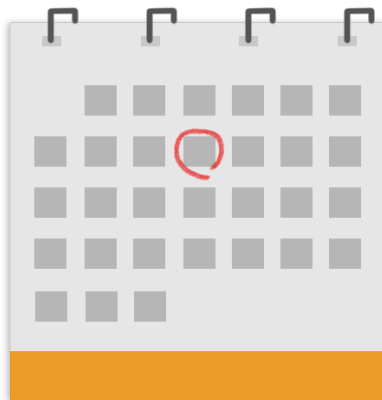


Educating staff about the risks

Planned staff training (CPD)

Have frequent safeguarding training so that all staff are equipped to identify children who may need help or support – and be familiar with the process to report any concerns. A reminder of any new or existing legislation and a recap of escalation processes is also useful to ensure everyone has the most up-to-date information.

Where possible, schools should try to engage parents in online safety training to empower them with the knowledge and skills to support their children at home.



Ad hoc meetings

It's important that staff are able to assemble meetings at short notice to discuss and share any concerning topics that are trending, ensuring that everyone is fully informed about current online safety issues.

[Learn more](#)  *ISTE Standards: Education leaders*

Effective monitoring tools

In many countries, there are requirements in place for schools to effectively monitor and control what students are doing online, both in supervised and unsupervised environments. These include **KCSIE**, **CIPA**, **ISTE** and so on. To fulfil this duty, schools need to go beyond just using internet metering.

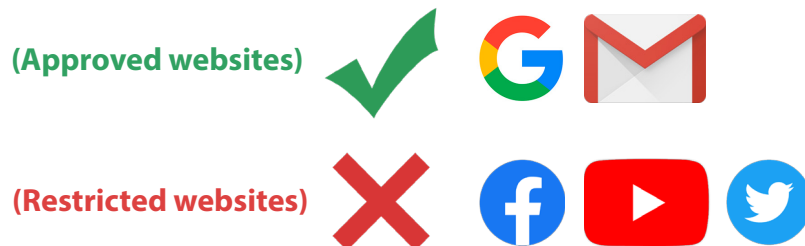


Internet filtering and monitoring is just the start

When it comes to internet filtering, sometimes it's best not to blanket ban everything.

1. It doesn't allow students the opportunity to learn about the safe and responsible use of the internet (aka, digital citizenship) in a controlled environment.
2. It doesn't provide the flexibility to allow specific websites to appear for particular age groups: i.e. Facebook access for Business Studies students studying marketing tools.
3. Overall, blocking access does nothing to safeguard the student because, in the majority of cases, nobody knew that access was being attempted in the first place.

In the same way, internet monitoring on its own doesn't provide context, which could mean schools are faced with a backlog of false alerts or are missing the crucial details to understanding students' behaviour.



The full picture

Instead, schools could consider online safety tools that pair internet metering

with contextual analysis, e.g. [NetSupport DNA](#) or [classroom.cloud](#). In this scenario, key words that students may be typing, copying or searching for are displayed in a word cloud format (along with other insights), so staff can spot trending topics across clusters of students. If phrases pop up that they think may suggest bullying/harassing behaviour or place the student at risk, staff are better placed to take appropriate action.

Contextual analysis will also indicate the context in which the words were being used. For example, a triggered phrase being used in a Word document during lesson time would be perceived as a lower risk than if the same phrase were being used in a messenger app during lunchtime.

This analysis uses variables such as considering the surrounding search sentences, the devices used, time of day, and websites visited (including previous alerts triggered) to create a numerical risk index, based on the context and history of a student's activities. This helps school staff to identify genuine concerns and prioritise them accordingly.

Empowering students

Allowing students to report concerns they might have is also key to encouraging wellbeing and pupil voice. This type of tool is especially useful for those who feel uncomfortable speaking directly to a staff member, as it allows them to share their problems and get help from staff without having to approach them in person. In addition, providing them with independent access to a tailored list of safeguarding resources can

[Learn more](#)  further support their empowerment.

Sexting
Grooming Radicalisation
Cyberbullying
Abuse Self-harm
Suicide Extremism



Actions for parents

Discuss online safety with your children

Talk to your child openly and regularly about the realities of what is posted online, as giving them the skills to make their own judgements is the only way to help keep your child safe. Sometimes, it's helpful to set boundaries on use and agree what's appropriate – and often it's useful to keep focused and talk about specific apps and websites that you can review together. Ask children what apps and sites they use and why. Another important conversation is understanding what a child feels is appropriate and then explaining possible risks in a clear and understandable way.

Open door policy

One of the more challenging areas to police is the forum-based chat capabilities within console-based games. These are often the hardest to manage. A simple “door open” policy when gaming at home can be a great start. Good practice is to also encourage the school IT department to provide regular updates to parents on tools that may support their efforts to keep their children safe online.

Communication with the school

In some instances, it may be appropriate to report back to the school a particular online safety issue that your child is going through or has experienced, as it may be a wider issue that others are facing and the school can help monitor the situation during school hours. Such cases should be handled confidentially and with sensitivity, depending on the nature of the topic, to avoid any further negative impact on the child.



[Learn more](#) ➔ *ISTE: How to talk to parents about learning technology.*

Summary

At school, staff can't be everywhere at once and technology can never be a replacement for eyes and ears. Yet, with appropriate online safety tools and policies in place, and with the reinforcement of digital citizenship messages alongside parental involvement, opportunities for online safety issues to be noticed and dealt with constructively are maximised.

Inside the school, with the help of **comprehensive technology**, any concerning online activity and trends can be flagged early on, allowing the appropriate designated staff to identify, educate and support their students. Equally, with good digital citizenship skills, children are equipped with the knowledge to make safe online decisions - whether they are inside or outside the school.

Glossary

Term	Definition
BICS	Term used by County Lines drug dealers when referring to the vulnerable young people recruited to sell drugs. It refers to them being disposable, like a BIC biro.
Black mollies	Slang term for amphetamines, also known as speed.
Blue Whale Challenge	Suicide game. A series of tasks assigned to players by administrators over a 50-day period, with the final challenge requiring the player to commit suicide.
Boost and shoot	Stealing to support a drug addiction or other habit.
Bullying	Hostile behaviour that is unsolicited (physical, social and verbal).
CCE	Child Criminal Exploitation.
Cinnamon Challenge	Online game. Eating a spoonful of ground cinnamon in under 60 seconds without drinking anything.
Costume make-up	Used to cover up or hide self-inflicted wounds/injuries with cosmetics.
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.

CSA	Child Sexual Abuse.
CSE	Child Sexual Exploitation.
Cupcaking	To flirt with someone online, not always with the best of intentions.
Cyberbullying	Bullying that has moved to the internet.
Cyberchondria	Cyberchondria refers to a person's anxiety about their health that is created or exacerbated by using the internet to search for medical information. A British newspaper coined the term in the early 2000s as a play on the word hypochondria.
Desensitisation/ Normalisation	Desensitisation or normalisation is a psychological process that has often been involved in explaining viewers' emotional reactions to media (games, internet viewing, other online media) violence and other acts. This logic may be applied to the effects of repeated exposure to media violence.
Digital self-harm	The practice of being mean to yourself online.
Doki Doki (Doki Doki Literature Club)	Video game. After a period of time playing, the young female characters start killing themselves and, during this process, suicidal images are shown.
Drunkorexic	Skipping meals in order to save calories to drink alcohol.
EDNOS	Acronym for: Eating Disorder Not Otherwise Specified. Typically given to someone whose symptoms do not meet all of the criteria for anorexia or bulimia.
End it all	Suicide indicator. Cry for help.
Fire Fairy	Online game. A social post will tell young girls to turn on the gas burners on their stove and repeat 'magical words' to become a 'fire fairy'.
FOMO	Fear Of Missing Out. Social anxiety stemming from the belief that others might be having fun without you.
GAD	Generalised Anxiety Disorder.
Grooming	To build a relationship, often with a young vulnerable child, with a hidden objective of sexual abuse or engaging them in criminal activity.
Homophobic	Dislike of or prejudice against the LGBT community.
KIK Dirty	A forum that promotes the sharing of explicit images.

Loot box	Virtual treasure chests containing items that can be used in games. Many games use psychological techniques borrowed from the gambling industry, ‘nudging’ players to keep spending money.
Momo	Online game. Children text a number on WhatsApp that then sends them instructions to complete a series of tasks which escalate.
My Secret Family	Reference to the hashtag #mysecretfamily that is part of a secretive language commonly found on Instagram, alongside posts relating to self-harm and suicide.
N4N	Nudes for Nudes. Used when asking someone to share inappropriate photos.
Neknomination	Online drinking game. Also known as ‘neck and nominate’. It’s when a person drinks a pint of an alcoholic beverage in one gulp.
Netflix and chill	Term popularised among young people in modern social media culture that can mean casual sex.
Nootropics	Also known as Smart Drugs. A group of drugs that improve cognitive function and memory and as such there is a growing trend for students to use these to aid studying.
NSSH	Non Suicidal Self Harm. Deliberately harming oneself without suicidal intent.
Online disinhibition	The loss of inhibitions that can stem from not speaking to people directly whilst using online platforms. This can lead to people being more confrontational, abusive and reacting in ways that they might not normally do in real life because they are online.
Online slots	Suggests the person is using online gambling sites, which could lead to an addiction.
Orthorexia	A compulsion to eat healthily. Many sufferers avoid social eating or food they have not prepared themselves and increasingly isolate themselves.
Phishing	An attempt to obtain sensitive information or data.
Pic 4 Pic?	Can be used to ask for nude images in exchange for nude images of the other contact.
Planet Suzy	Online forum for sharing and finding explicit imagery.
Pro Ana	The promotion of behaviours related to the eating disorder anorexia nervosa.

Racist	Person who is prejudiced against people on the basis of their membership of a particular racial or ethnic group.
Radicalisation	A process by which an individual or group comes to adopt increasingly extreme political social or religious ideals and aspirations.
Salt and Ice Challenge	Online game. Putting salt and water on your skin, then seeing how long you can hold a piece of ice against it to create a skin burn.
Sexting	Sending sexually explicit messages, photos or videos via a digital device.
Silhouette Challenge	A TikTok challenge where participants apply filters to videos and dance provocatively in silhouette.
Skinny Me	Commonly a social media term referring to detox products and achieving the perfect body image.
Spamming	The use of messaging systems to send unsolicited messages.
Struggling to cope	An indicator of depression and anxiety. A cry for help.
Suicidal	Cry for help, sign of depression. Someone who is considering suicide.
Thigh gap	The space between the inner thighs when standing upright with knees touching. Has become an aspect of physical attractiveness in modern society.
Thinspiration	Something or someone that serves as motivation for a person seeking to maintain a very low body weight.
Trapping	Can refer to the act of moving drugs from one town to another or selling drugs.
Trashing site	Online forums dedicated to trolling people with a prominent online presence.
Upskirting	A practice where illicit photographs are taken under the victim’s clothing without their knowledge, usually for the purpose of sharing on social media.
Viral	An image, video, or link that spreads rapidly through a population by being frequently shared online.
YODO	You Only Die Once.

¹ Riehm, K.E., Feder, K.A. & Tormohlen, K.N. (2019). Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among U.S. Youth. JAMA Psychiatry. Published online September 11, 2019. doi:10.1001/jamapsychiatry.2019.2325

² Bloom, M. Constructing Expertise: Terrorist Recruitment and “Talent Spotting” in the PIRA, Al Qaeda, and ISIS. Stud. Confl. Terror. 2017, 40, 603–623.



Online Safety Guide

2022

www.netsupportdna.com
classroom.cloud

