ONLINE DIGITAL SAFETY AWARENESS

ADVICE GUIDE ON HOW TO STAY SAFE ONLINE & MOBILE

A LITTLE HISTORY

VOICE was launched in 2019 to help enhance the life of young people from disadvantaged backgrounds and areas with a higher level of poverty.

We trace our humble origins to our first ever youth club in the Southall area of West London, providing a safe environment for young people to meet new people, engage in fun activities, events, inspirational talks and educational workshops.

Our aim is to give young people the opportunity to develop their personal and social skills and empower them to participate in society as mature and responsible individuals.

Since 2019 we have branched out to Slough, Hayes, Watford & Leicester. VOICE also offers a 24 hour helpline and a referral system where young people or concerned parents can find support and advice on any issues they maybe facing.

DIGITAL SAFETY

As more APPs are readily available we have produced this information booklet that highlight the most common apps young people use the dangers and how to monitor and protect your child on social media.

WORKING IN PARTNESHIP WITH

Khalsa Fostering
every hand can make a difference

www.khalsafostering.co.uk

SIKH RECOVERY NETWORK

www.sikhrecoverynetwork.org

KIRPA THERAPY

www.kirpatherapy.com

CONTENTS

4 - PARENTAL CONTROL (ANDROID)
5 - PARENTAL CONTROL (I-PHONE)
6 - ONLINE GROOMING
7 - CYBERBULLYING
8 - FRIENDS & FOLLOWERS
9 - LOCATION TRACKING
10 - EMAIL SCAMS
11 - FACEBOOK
12 - WHATSAPP
13 - INSTAGRAM
14 - TWITTER
15 -YOUTUBE
16 - SNAP CHAT
17- HOOP FOR SNAP CHAT
18 - TIK TOK
19 - TOP TIPS FOR PARENTS

VOICE
every voice needs to be heard!

WE NEED YOUR HELP!
MAKE A DONATION TODAY!

Every donation we receive helps us sustain our projects. Every call we answer, every referral we take, every workshop or session we conduct helps protect children today and prevent abuse from happening tomorrow.

We cannot run our projects or sustain them without your continuing support – whether volunteering for us or making a regular donation. Your efforts could help safeguard a vulnerable child and give them a brighter future.

Donate Online Visit: www.voicehelpline.co.uk

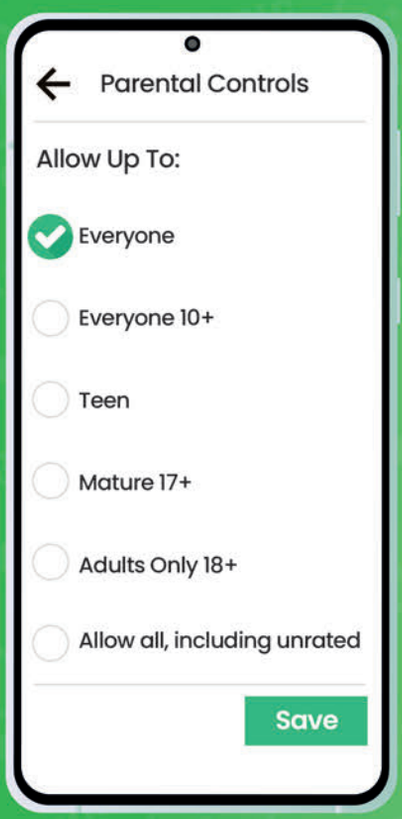
SCAN QR TO MAKE A DONATION

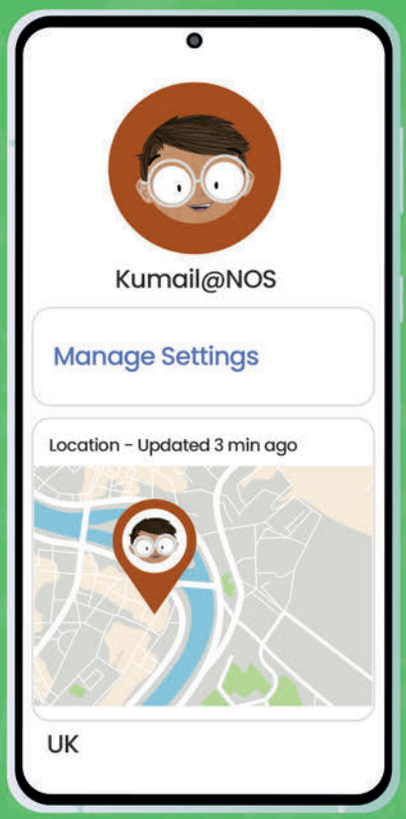
National Online Safety®
www.nationalonlinesafety.com

How to Set up PARENTAL CONTROLS to limit age-inappropriate CONTENT

Android Phone

The settings on an Android device allow you to prescribe certain rules for when your child is using it. For example, you can block specific types of content to reduce the risk of your child being exposed to age-inappropriate material (music with explicit lyrics, for instance, and games, TV shows or movies that are unsuitable for young people). There are two ways to access parental controls on an Android phone: through Google Play or via the Google Family Link app. You can also lock your changes behind a PIN, so your child (or anyone else) can't change them back.





Set up parental controls with Google Family Link

1. On your phone, install Google Family Link for Parents
2. Tap Open and review the information
3. Tap Get Started
4. Tap Next to set up your child's device
5. On your child's phone, download Google Family Link for Children & Teens and enter the Family Link setup code provided
6. On your phone, open the Family Link app
7. Tap your child's name
8. Tap Manage Settings
9. Tap Controls on Google Play
10. Tap the content you would like to restrict
11. Choose how to filter or restrict access

Set up parental controls with Google Play

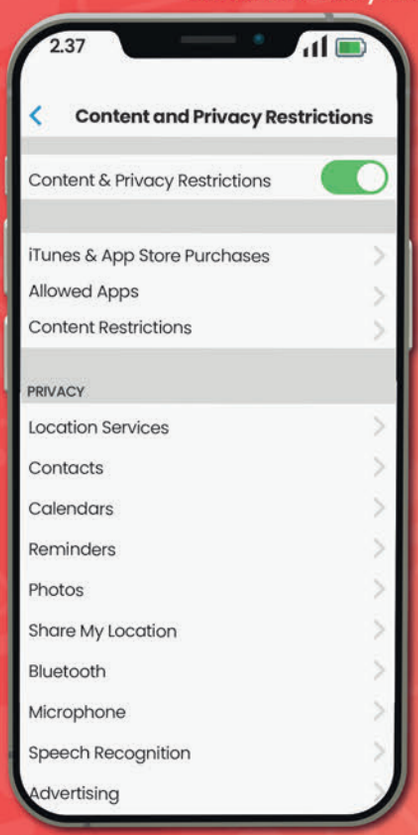
1. Open the Play Store app
2. Tap Menu (represented by three horizontal lines)
3. Tap Settings
4. Tap Parental Controls
4. Enable Parental Controls
4. Create Pin
4. Tap the content you would like to restrict
4. Choose how to filter or restrict access

How to Set up PARENTAL CONTROLS to limit age-inappropriate CONTENT

iPhone

National Online Safety®
www.nationalonlinesafety.com

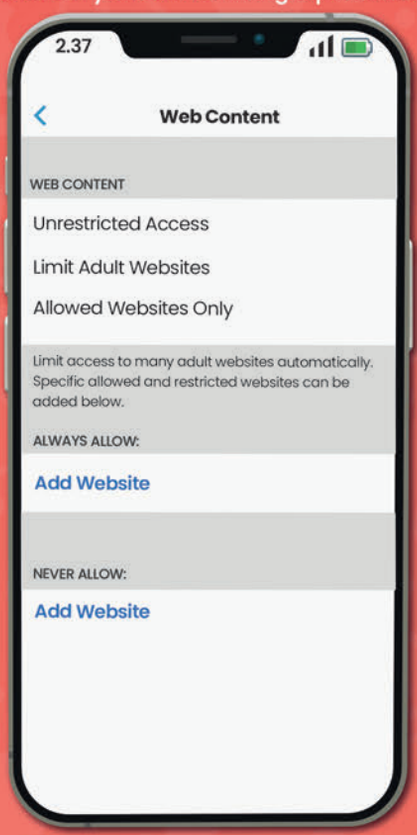
The parental controls on iPhones allow you to block or restrict certain apps, features, content, downloads, or purchases. Setting limitations on content ratings, Siri and web searches enables you to filter out age-inappropriate content and vastly reduce the likelihood of your children being exposed to unsuitable material and information.



Set up content rating restrictions

Content filters keep your child from viewing unsuitable material. They block apps, films and TV shows with specific age ratings, and music and podcasts with explicit content.

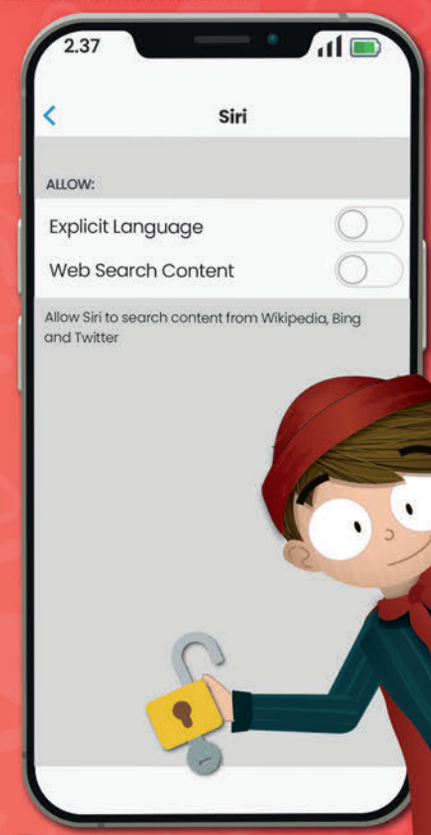
1. Open Settings
2. Tap Screen Time
3. Enable Content & Privacy Restrictions
4. Tap Content Restrictions
5. Choose the Settings for each feature you which to restrict



Set up web restrictions

Website content filters restrict age-inappropriate content on Safari. You can also blacklist certain websites or allow access only to approved sites.

1. Open Settings
2. Tap Screen TIme
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions
4. Tap Web Content
5. Choose between Unrestricted Access, Limit Adult Websites and Allowed Websites Only
7. Choose which websites you wish to allow/block



Set up Siri web search restrictions

You can screen out explicit language to avoid Siri displaying inappropriate results. You could also disable Siri entirely, so your child can't use it to search the web.

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions
5. Scroll Down to Siri
6. Choose to block either or both Web Search Content and Explicit Language

Online Grooming is when someone befriends and builds an emotional relationship with a child and communicates with them through the internet with the intent to commit a sexual offence. This type of victimisation can take place across any platform; from social media and messaging apps to online gaming and live streaming. Often it involves young people being tricked, forced or pressured into doing something they wouldn't normally do (coercion) and often the groomer's goal is to meet the victim in a controlled setting to sexually or physically abuse them. In some cases children may be abducted or have long-lasting psychological damage.

What parents need to know about

ONLINE GROOMING

CHILDREN ARE MOST VULNERABLE

Unsurprisingly children are often most at risk as they are easy to target and unlikely to question the person who is engaging in conversation with them. Groomers will use psychological tricks and methods to try and isolate them from their families and friends and will often choose to target more vulnerable children who may be easier to manipulate. Predators will stalk apps and websites that are popular with young people and will use a 'scattergun' approach to find victims, contacting hundreds online to increase their chances of success.

LIVE STREAMING CONCERNS

Predators may use live video to target children in real-time using tricks, dares or built-in gifts to manipulate them. Grooming often takes the form of a game where children receive 'likes' or even money for performing sexual acts. Social media channels, such as YouTube, Facebook, Instagram and Snapchat, all have live streaming capabilities, but there are many apps which children can use to live stream, including Omegle, Live.me, BIGO Live, YouNow and many more

ANYONE CAN BE A PREDATOR

The internet has made the ability to interact with strangers online easy. Many sites and apps are reliant on individual users entering their own information when signing up. However individuals can remain anonymous if they choose to enter inaccurate information and many online predator cases are due to groomers using impersonation techniques. However, often the greater threat comes from adults who 'hide in plain sight', choosing to befriend young children without hiding their real identity.

CAN BE DIFFICULT TO DETECT

Unfortunately, most children find the 'grooming' process (before any meeting) an enjoyable one as the predator will compliment, encourage, and flatter them to gain their trust, friendship and curiosity – 'a wolf in sheep's clothing' scenario. This often means children fail to disclose or report what is happening. If the groomer is also previously known to the child, their family and their friends, then this can make detection even harder.

FROM OPEN TO CLOSED MESSAGING

Online predators may contact their victims using any number of ways including social media, forums, chat rooms, gaming communities or live streaming apps. Sometimes there is little need to develop a 'friendship /rapport stage', as the victim has already shared personal information online and is communicating openly with others. Children may also be prepared to add other online users they don't know so well to gain 'online credibility' through increasing their friends list. Predators will often seize this opportunity to slowly build a relationship and then move their conversation with the child to a more secure and private area, such as through direct messaging.

EMOTIONAL ATTACHMENTS

Online predators will use emotive language and aim to form close, trusted bonds with their victims through showering them with compliments and making them feel good about themselves. Often victims will refer to them as their 'boyfriends' or 'girlfriends' and it can be difficult to convince some young people that they have been groomed, often leading to lasting psychological effects.

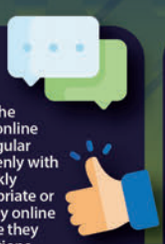
National Online Safety®

#WakeUpWednesday

Safety Tips for Parents & Carers

IT'S GOOD TO TALK

It's unlikely that you can stop your child using the internet, nor can you constantly monitor their online activities, but you can talk to your child on a regular basis about what they do online. By talking openly with them about online relationships, they can quickly ascertain the kind of behaviour which is appropriate or inappropriate. Ask them whether they have any online friends or if they play online games with people they haven't met. This could then open up conversations about the subject of grooming.



CHECK PRIVACY SETTINGS

In order to give your child a safer online experience, it is important to check privacy settings or parental controls on the networks, devices, apps, and websites they use. Disable location sharing if you can. If you use location-sharing apps to check where your child is, remember that these could always be used by strangers to follow your child without their knowledge. Ensure that you check options so that location information is never shared with anyone except those they have permission to share with.

MONITOR SOCIAL MEDIA & LIVE-STREAMING USE

It's important to be aware of what your child is sharing on social media and with whom. Create your own profile and become "friends" with them or follow them so that you can monitor their activity. Similarly, always check on them if they are live streaming and implement privacy controls. Choose a generic screen name and profile picture that hides their identity. You may also feel more comfortable being present each time they live stream.

STICK TO 'TRUE FRIENDS'

Make it clear to your child that they should not accept friend requests from people they don't know and to verify friend requests with people who they do know. Encourage them to only interact and engage with 'true friends' i.e. those friends who don't ask personal questions such as close family and friends. Remind them to never agree to chat privately with a stranger or someone they don't really know and to never divulge personal information, such as mobile phone numbers, addresses, passwords or the name of their school.

DISCUSS HEALTHY RELATIONSHIPS

Talk to your child about what a healthy relationship looks like and how to detect someone who might not be who they claim to be. Explain that groomers will pay your child compliments and engage in conversations about personal information, such as hobbies and relationships. They may admire how well they play an online game or how they look in a photo. Groomers will also try and isolate a child from people close to them, such as parents and friends, in order to make their relationship feel special and unique.

BE SUPPORTIVE

Show your child that you will support them and make sure they understand they can come to you with any concerns they may have. They need to know they can talk to you if someone does something they are uncomfortable with, whether that is inappropriate comments, images, requests or sexual comments.

Meet our expert

Jonathan Taylor is an online safety expert and former Covert Internet Investigator for the Metropolitan Police. He is a specialist in online grooming and exploitation and has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, social media apps and platforms.

LOOK OUT FOR WARNING SIGNS

Child safety experts have identified key grooming patterns and advise parents to look out for:

- Secretive online behaviour.
- Late night internet or smartphone usage.
- Meeting new friends in unusual places.
- Becoming clingy, develop sleeping or eating problems or even bedwetting.
- Lack of interest in extra-curricular activities.
- Having new items, such as clothes or phones, unexplainably.
- Seem withdrawn, anxious, depressed or aggressive.
- Having older boyfriends or girlfriends.

The Diana Award definition of bullying is "repeated negative behaviour that is intended to make others feel upset, uncomfortable or unsafe." Cyberbullying is bullying which takes place online. It can involve anything from sending messages to posting offensive comments to uploading and sharing private or embarrassing photos. It is classed as an indirect form of bullying when compared to verbal or physical bullying, given it usually takes place through a digital device. However, for those experiencing bullying behaviour, the consequences can be just as serious and have far reaching effects.

What schools need to know about CYBERBULLYING

3 KEY ASPECTS OF BULLYING BEHAVIOUR

There are three key aspects of bullying behaviour, namely that it is repetitive, negative and intentional. These behaviours apply both offline and online. Cyberbullying can almost heighten these behaviours, particularly with access to the internet available 24/7 and the different ways in which those displaying bullying behaviour online can target others. The fact that they can also easily hide their identity online can make cyberbullying much more difficult to stop.

DIFFERENT DEVICES & CHANNELS

Cyberbullying can take place over any device connected to the internet which allows for two-way communication. This includes mobile phones, tablets, computers and even games consoles as it becomes more and more common for players to chat to other players whilst playing online. From a snapshot of 1,400 students surveyed by the Diana Award in 2018, 33% of young people admitted to have experienced bullying on social media, 11% via text message and 12% whilst online gaming.

WHAT LEADS TO CYBERBULLYING

There is never any justification for cyberbullying and those who display bullying behaviour need to be held to account for their actions. Nonetheless, it can useful to try and understand some of the factors that may lead young people into bullying behaviour. For example, family issues, personal difficulties and a lack of positive reinforcement may push some young children into bullying others as a form of coping mechanism. Similarly, those exhibiting bullying behaviour may blame their targets for provoking their behaviour in the first place or engage in bullying behaviour as a call for attention if they lack social skills or understanding. Others may view their position as dominant which makes themselves less vulnerable to being bullied or they replicate behaviour they have experienced themselves in the past.

SIGNS AND SYMPTOMS

Cyberbullying can affect anyone, at any time, at any place. The impacts of cyberbullying can be long-lasting and leave people feeling scared, anxious and lonely. Some of the more obvious signs that those experiencing bullying behaviour might show include weight loss, crying, mood changes, depression and regularly avoiding school. Other symptoms, which might be less obvious to spot and would be difficult to pick up on in isolation, may include changes in body language like hunched shoulders, walking slower or an inability to make eye-contact. In extreme cases, those experiencing bullying behaviour may have unexplained marks or scars which could be evidence of self-harm.

National Online Safety®

#WakeUpWednesday

Tips for School Staff

TAKE A WHOLE SCHOOL APPROACH

In taking a whole approach towards cyberbullying, schools can cultivate a culture that relies on positivity and behaviour that is emulated by ALL members of the school community including staff, support staff, senior leaders, governors and parents and carers.

BUILD CONFIDENCE IN DEALING WITH INCIDENTS

This can be achieved by having clear knowledge of what constitutes bullying behaviour, having clear sanctions and courses of action and continually updating your knowledge of safety procedures regarding online and offline incidents.

USE CHILDREN AND YOUNG PEOPLE AS A RESOURCE

Ensure you understand what is influencing the behaviour of young people in your community. If schools know what their students are engaging with, it can be easier to develop and implement relevant and effective tactics / strategies to counter cyberbullying issues.

UNDERSTAND THE CAUSES OF BULLYING

As previously mentioned, sometimes those who are behind the bullying are in need of support just as much as those who being targeted. In better understanding the cause of the issue, schools can better position themselves to tackle the problem and also adequately support both those displaying and experiencing the bullying behaviour. Taking a proactive approach means that schools can gear themselves to tackle issues specific to their school environment, rather than treating each case the same.

ENSURE ALL STAFF KNOW THEIR ROLES AND RESPONSIBILITIES

All staff have a role to play in educating and supporting children who are affected by cyberbullying, not just those responsible for safeguarding or online safety. Regular training, continuous professional development and clear school policies can help to empower staff in effectively managing any cyberbullying issues and in providing a united staff front on zero tolerance to all bullying behaviour.

Ask For Help

For further support, advice or guidance to support you students at school, or to sign up to our FREE Anti-Bullying Ambassadors training events, head to www.antibullyingpro.com

Part of our Social Media & Live Streaming Series

NOS Social Media & Live Streaming

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

FRIENDS & FOLLOWERS

What are they?

'Friends & Followers'

What makes social media actually 'social' are the connections users make with other users on the platforms. Every social networking site handles these connections differently, calling them 'connections', 'friends' and 'followers', amongst others. Having friends and followers is how we find out what other people say and do. Your friends and followers are much more likely to see your online content than those outside of your network, which is why it's important to be mindful of who you connect with and what you share. On some platforms, if two accounts follow each other, this may allow additional communication channels such as private messaging.

Know the Risks

Access to private information

This may include your child's home address, school, date of birth, names of siblings or other relations, as well as seeing photos that inadvertently contain sensitive information. This is completely harmless information for genuine friends or family but could cause issues in the hands of a criminal.

Catfishing

'Catfishing' is the common name given to an individual posing as someone else on social media. They do this to try and befriend typically young and vulnerable people who they look to then take advantage of. Unfortunately, there are many examples of this happening across the world that have had real-life consequences.

Online bullying

Once a connection is made on social media, there is the potential to send private messages between individuals. It is difficult for social networks and other users to see what is being said between accounts. This provides an opportunity for bullies to victimise individuals and can create a dangerous spiral of online activity.

Safety Tips

Check privacy settings

Platforms such as Facebook allow users to modify their privacy settings, which means people who are not friends can't see all your profile information. It's also possible to hide this information for some or all of your connections. Always make sure your child's accounts are set to private.

Talk about strangers

Make sure children understand that they should only connect with people that they know or can completely trust. They should be wary of anyone messaging them frequently who they don't know in real life or have never spoken to or actually seen online. Catfish will stick to text-based messaging only, to keep their identity secret.

Delete old connections

Children should be mindful that everything they share will probably exist online forever and that they shouldn't share anything that gives too much information away. Every now and again, they should delete old connections that they no longer spend time with. Old accounts can easily be hacked, exposing personal information to strangers.

Further Support

Encourage an open dialogue

It's really important that your children knows that they can speak to someone about anything they're not sure of online. It's crucial that they know they won't be judged or told off for anything they've done; it's far more important to know if they're in danger or worried about something.

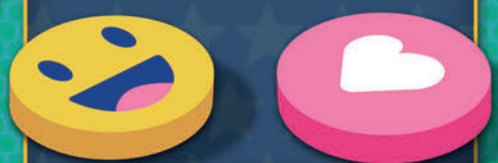
Seek additional guidance

If your child wants to spend a lot of time online and is displaying compulsive or addictive behaviour, is negative, struggles with schoolwork and reduces real-life interactions or has frequent changes in mood, they could be experiencing negative interactions online. Speak to them and seek support from their school or your local safeguarding team if you think your child has been affected.

Our Expert

Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.



Part of our Online Relationships Series

NOS Online Relationships

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about...

LOCATION TRACKING

What is it?

'Location Tracking'

Location tracking has always been a fundamental part of the way mobile phones work, the most basic element of which is the ability to triangulate a device's position in relation to a mobile network's radio masts. As smartphones became popular, Global Positioning System (GPS), Wireless networking (Wi-Fi), and Bluetooth Low Energy (BLE) technologies complemented this, any one or combination of which can now feed highly accurate location data via any app on that device.

How Does it Work?

Based on consent

In the UK, data protection laws require that access to a person's personal data (including their location) is based on consent. In principle, the same protection applies to children even when parents use location tracking to keep tabs on them although this is a grey area for under-16s.

Location sharing apps

As well as being built into Google's Android and Apple's iOS software, location sharing is often a feature of popular apps, for example Snapchat's Snap Maps, specifically designed to appeal to children, or WhatsApp Live Location. These usually require the user to turn the feature on.

Wi-Fi surveillance

Although location tracking is associated with GPS, in urban areas Wi-Fi is more important. Tech companies have built up highly accurate pictures of the location of Wi-Fi networks in towns and cities. As a smartphone moves within range of these networks, it's possible to accurately calculate that device's location.

Know the Risks

Non-consensual monitoring

Whilst location tracking has many benefits, a number of apps have recently emerged that allow location data to be sent to third parties. This inevitably raises the risk of location tracking via apps being used, without consent, to keep tabs on someone's whereabouts.

Frequently visited locations

A function of mobile operating systems is to document location history, which can provide someone with access to all past locations a child may have visited since location permission was granted. Anyone with access to a child's phone could establish where they go and when an build up a pattern of where they are likely to be at any particular time of the day.

Stalking apps

Whilst these apps are often illegal, gathering evidence for prosecutions can be difficult. Stalking apps are designed to monitor someone's smartphone communication and location without their knowledge or consent and could be used as part of harassment or stalking activity.

Safety Tips

Disable when not in use

It's possible to turn off or limit location sharing on mobile devices, but this will also disable other features such as street navigation. It may be better to explore which apps are using location sharing and in what ways and that young people know to turn if off when the app is not in use.

Discuss the risks

Young people are often unaware that location sharing is powerful and open to abuse. Talk to them about how it can be misused and discuss the importance of keeping their data private. Tell them to never provide others with unauthorised access to their phone and to always keep it locked when not in use.

Talk about location monitoring

Remind children that smartphones are a powerful technology that can monitor and record everywhere a person goes as well as all their communication. Talk about the law and about what they can and can't do to others and that monitoring someone else's location without their consent is a huge invasion of their privacy.

Our Expert

John Dunn

John E Dunn is a hugely accomplished cybersecurity expert who has edited and written for numerous computer and technology magazines since the early 1990s, most recently Which Computing, The Register, Computerworld and Naked Security. He is the co-founder of Techworld and has featured on BBC TV/radio as well as CBC Canada.

What Parents & Carers Need to Know about EMAIL SCAMS

Email scams are when you receive a mail from someone purporting to be a genuine person or company, but is actually an online fraudster trying to trick you into disclosing personal information. This is often referred to as 'phishing'. Normally, people click on the links in an email assuming that they will be directed to a trustworthy website – but fake sites, closely resembling the real thing, are increasingly being set up by cyber criminals specifically to capture your personal information, which could in turn jeopardise your financial, emotional and possibly even physical wellbeing.

Disguised Deceptions

Some scam emails can appear to be from companies that you know and use. For example, you could receive an authentic-looking email advising of a problem with your account or payment method. Instead of reacting to the email and disclosing personal information like bank details, it's wise to call the company directly on a trusted number to confirm if there actually *are* any account issues.

Identity Theft

Another significant risk is falling victim to identity theft. If a scammer manages to acquire your usernames and passwords, they would then have access to your online accounts – and they could effectively pretend to be you. This could have a massive negative impact if changes were made to your accounts, for instance, or the scammer communicated with your contacts while posing as you.

Viruses and Malware

A particularly devastating hazard with scam emails is that some links, when clicked on, could result in dangerous viruses or malware being downloaded onto your devices. This could enable scammers to harvest valuable information without your consent (and sometimes even without your knowledge) or prevent you from accessing the device altogether, making it unusable.

Financial Damage

One of the primary consequences for victims of an email scam is the financial cost. If you *do* click on a scam email and disclose any personal information, it can then be used to take money from accounts belonging to you and your family. Depending on exactly what information the cyber criminals obtain, this could result in significant and far-reaching financial losses and personal stress.

Hijacked Accounts

A scammer with access to your accounts could – once they're logged in as you – deny you entry. If they were to change the password, it would – in most cases – not allow you any further access. Even for accounts with little or no financial value attached, this could be hugely inconvenient: you could permanently lose data and files that you had invested a considerable amount of time in.

Personal Safety

Another danger of scam emails is that, in extreme cases, they could ultimately lead to a threat to your physical wellbeing. If someone is demanding to meet with you and has accessed your personal information (your address, for example), they could attempt to confront you in person – which is of course exceptionally dangerous. Losing control of sensitive information could put you in a vulnerable position.

Advice for Parents & Carers

Protect Personal Details

Never input any personal information into websites that you are unfamiliar with. If you were redirected onto a certain page by clicking a link in an email, entering your personal details could then give away your location or other key information to the scammer. This could then put you in physical danger as the cyber criminals would know exactly where to find and approach you.

Beware of Suspicious Emails

If you are unfamiliar with the sender, it's safest to simply not open an email. When an email makes you wary, mark it as junk (to reduce the chance of any recurring issues) and then delete it. Awareness of phishing is the primary method of defence against malicious emails. Once someone knows how to identify and deal with scam emails, they are far less likely to fall prey to them in future.

Check Spelling and Grammar

Pay close attention to any spelling mistakes or grammatical errors. Many scam emails can be spotted this way, as they often tend to contain these types of mistakes. Make sure your child knows that if they *do* spot this sort of tell-tale error and is not sure who the email came from, it's a good idea to either delete the email or report it to a trusted adult to prevent any possible future harm.

Access Sites Manually

If you or your child wish to visit a particular website, it's safest to avoid clicking on a link in an email to take you there. Instead, find the site through your search engine or manually type the address into your browser. This significantly reduces the possibility of being redirected to a bogus website where fraudsters could capture your personal information after you enter it.

Don't Open Dubious Attachments

If you or your child ever see any files as attachments on emails that you are uncertain about, do not download them or even click on them: this could result in your systems being infiltrated. If your devices at home do not already have anti-virus software, you should install some and ensure it is regularly updated. This will help you to detect and remove any dangerous files as soon as possible.

Meet Our Expert

Formed in 2016, KryptoKloud provides cyber security and resilience solutions to its customers. With offices in the UK, the company offers managed service operational packages including cyber security monitoring and testing, risk audit, threat intelligence and incident response.

KryptoKloud

National Online Safety®

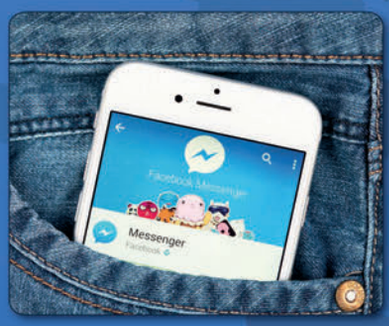
#WakeUpWednesday

SOURCES:
https://www.infosecurity-magazine.com/news/education-disproportionate-spear/, https://www.impactmybiz.com/blog/cybersecurity-in-education-stats-2020/

Facebook Messenger is a communication and chat application which is part of the wider Facebook platform and has been a standalone app on mobile devices since 2011. Through Messenger, users can exchange messages and send photos, videos, stickers, gifs, audio files and play games. It allows both one-to-one conversations and group chats, has a 'stories' feature and provides the ability to set up a video call session with up to 50 people at a time through its latest update, Messenger Rooms. That's why we've created this guide to help parents and carers understand exactly what Facebook Messenger is all about.

AGE RESTRICTION
13+
Anyone over the age of 13 can create an account

What parents need to know about FACEBOOK MESSENGER



ADDICTIVE NATURE

Whereas Messenger is integrated into Facebook itself on a desktop or laptop, it is a separate app on mobile phones. It is similar in many ways to other messaging platforms with the added bonus of being able to upload stories, make live video calls and have group chats, beyond just standard text messaging. All of this can encourage children to spend more time on the app and on their phone, contributing towards increased levels of screen time.

REQUESTS FROM STRANGERS

Messenger cannot work without creating a Facebook account first. From here, if your child sets their profile to public, there is a chance that children may receive message requests from people they don't know. There have been reports of online grooming on Facebook and some people use fake profiles to reach out to children they don't know to try and encourage them to engage in conversation.

SECRET CONVERSATIONS

Messenger has a function called 'Secret Conversations' which means that your child can have encrypted end-to-end conversations with another user. Unlike regular chat on Messenger, these messages can only be viewed on the device being used and are not transferred to anywhere else where Messenger is logged in. Messages can also be set to delete after a time, although screenshots can still be taken. This means your child could engage in a private conversation with someone, who may look to take advantage of them, but leave no record of any previous messages.

LIVE STREAMING RISKS

LIVE

Through its latest feature, Messenger Rooms, Facebook now offers the ability to hold live video calls with up to 50 different users. Although video calls aren't new on Messenger, this latest addition pushes the 'live streaming' element of the app, which is also linked to WhatsApp and Instagram, and doesn't necessarily require a Messenger account. This can heighten the risk factors around privacy, security and being exposed to explicit or inappropriate content from other users with little, to no, prior warning.

OVERSHARING PERSONAL INFORMATION

Messenger can be an easy way for children to overshare personal or sensitive information with people they don't know. If Messenger is granted access to their photo library, links a phone number to the account or enables location settings, children can potentially share their private photos, videos, mobile number and even their current location with others.

TARGETED ADS & DATA SCRAPING

Facebook uses algorithms to understand how users interact with their platform and also what they're interested in. Messenger is not immune to this, and data shared - even between your child's friends - can be used to target children with advertisements around topics such as health, fitness, beauty, celebrities or something else which might not always be age-appropriate.

AD

CYBERBULLYING RISKS

#BULLY

Like many other social media platforms or messaging apps, Messenger can be an avenue for cyberbullies or trolls to target children through online abuse or sending nasty private messages. This might be in the shape of harassment from others or being purposely excluded from or targeted in group chats.

NOS National Online Safety®

#WakeUpWednesday

Safety Tips for Parents & Carers

REPORT INAPPROPRIATE BEHAVIOUR

If your child experiences anything negative on Messenger or is sent content from someone which makes them feel uncomfortable, they should speak to you about it and report it directly to Facebook. Users can also be blocked from messaging your child further and if your child doesn't want to display to others that they are online, they can switch off their active status from the settings.

KEEP YOUR PROFILE & STORIES PRIVATE

You can setup your child's profile on Facebook so that only friends can contact them. Similarly, on Messenger, parents can make their child's 'stories' feature only visible to their friends list. Not adding a phone number also means that your child can't be found by searching for their personal number. This helps to keep their account more secure and less likely to be found by people they don't know.

SHARE THEIR MESSENGER ACCOUNT

Some parents insist on checking their children's messages regularly, to see who they are talking to, rather than what they're talking about. This can seem intrusive, but when approached in a sensible, collaborative way, it can help you to keep an eye on who your child is communicating with and help to reduce the chances of misuse.

DISCUSS LIVE STREAMING RISKS

LIVE

Speak to your child about how to use video calls safely and securely. Make sure that when setting up video calls on Messenger Rooms, invites are only sent to friends and family that your child knows and only allow people into the 'room' who they trust. Discuss how they should behave and that they should act responsibly during a live stream, even if it is with people they know.

EXPLAIN THE DANGERS

Give examples of how Messenger has been used by other users pretending to be someone else to get information that they may do harm with. Tell your children that whilst Messenger is a great way for people to communicate and have fun, not everyone is who they claim to be and that they shouldn't accept messages from people they don't know and shouldn't share any private information, such as pictures, videos or their location, with strangers.

Meet our expert

Alex Wright is a former Facebook employee and social media expert with over 15 years' experience working in digital media. He has worked with some of the biggest organisations in the world and has a wealth of knowledge in understanding how social media platforms work and how they engage their audience.

SOURCES: https: //www.facebook.com/help/messenger-app/
https://www.androidcentral.com/how-make-facebook-messenger-secure-possible

What Parents & Carers Need to Know About WHATSAPP

16+ in UK & EU; 12+ rest of world.

WhatsApp is the world's most popular messaging service, with around two billion users exchanging texts, photos, videos and documents, and making voice and video calls. The app offers end-to-end encryption, meaning messages can only be read by the sender and the recipient(s). Not even WhatsApp can read them. Updates to its privacy policy in 2021 reportedly caused millions of users to leave the app. But the new policy was widely misinterpreted: it only related to WhatsApp's business features, not to personal messages.

'Prize' Scams

WhatsApp users occasionally receive messages from unauthorised third parties or fraudsters pretending to offer prizes – encouraging recipients to click a link to win. A common scam involves a warning that someone's WhatsApp subscription has run out: aiming to dupe them into disclosing payment details. Other scams include instructions to forward a message to earn a gift or reward.

Enabling Fake News

WhatsApp has unfortunately been linked to accelerating the spread of dangerous rumours. In India, some outbreaks of mob violence were reported to have been sparked by false allegations shared on the app. WhatsApp itself took steps to prevent its users circulating hazardous theories and speculation in the early weeks of the Covid-19 pandemic.

Connections with Strangers

To start a WhatsApp chat, you need the mobile number of the person you want to message (they also need to have the app). WhatsApp can also access the address book on someone's device and recognise which of their contacts use WhatsApp. If your child has given their mobile number to somebody they don't know, that person could then use it to get in touch via WhatsApp.

Disappearing Messages

With 'disappearing messages', users can send messages that vanish from WhatsApp after seven days. A new feature also erases photos and videos from chats after they've been viewed. These files can't be saved or forwarded on, making monitoring what children are discussing problematic – and if someone sent your child an inappropriate message, it would be difficult to prove. Content can be reported to WhatsApp, however: ensure your child knows how to do this.

'Only Admins' and Cyberbullying

Group chats and video calls are great for connecting with multiple people in WhatsApp, but there is always the potential for someone's feelings to be hurt by an unkind comment or joke. The 'only admins' feature gives the admin(s) of a group control over who can send messages. They can, for example, block people from posting in a chat, which could make a child feel excluded and upset.

Live Location Sharing

The 'live location' feature lets users share their current whereabouts, allowing friends to see their movements. WhatsApp describes it as a "simple and secure way to let people know where you are." Indeed, it *is* a useful method for a child to let loved ones know they are safe. But if your child is in a chat with people they *don't* know, it means they will be exposing their location to them, too.

Advice for Parents & Carers

Report Potential Scams

Advise your child not to engage with any message that looks suspicious or too good to be true. When your child receives a message from an unknown number for the first time, they will be given the option to report that number as spam. They can also report a contact or a group as spam by tapping on the contact or group name to open their profile and scrolling down to 'report spam'.

Explain about Blocking

If your child receives spam or offensive messages, calls or files from a contact, they should block them. Communication from a blocked contact won't show up on their device and stays undelivered. Blocking someone does not remove them from your child's contact list – they would also need to be deleted from the device's address book. The option to block someone is on their contact info screen.

Create a Safe Profile

Even though someone would need your child's phone number to add them as a contact, as an extra precaution it's worth altering your young one's profile settings to restrict who can see their photo and status. The options are 'everyone', 'my contacts' and 'nobody.' Choosing one of the latter two ensures their profile is protected.

Leave a Group

If your child is part of a group chat that makes them feel uncomfortable, or has been added to a group that they no longer want to be part of, show them how to use the group's settings to leave. If someone exits a group, the admin can add them back in once; if they leave a second time, it is permanent.

Use Location Features Sparingly

If your child needs to use 'live location' to show you or their friends where they are, advise them to share their location only for as long as they need to. WhatsApp gives 'live location' options of 15 minutes, one hour or eight hours. However, your child can manually choose to stop sharing their position at any time.

Delete Accidental Messages

If your child has posted a message in the wrong chat or sent a message that they immediately regret, they can delete it. Tap and hold on the message, choose 'delete' and then 'delete for everyone.' WhatsApp allows seven minutes to delete a message after it's sent – but it's important to remember that recipients may have seen (and taken a screenshot of) a message before it was deleted.

Fact-Check Messages

You can now fact-check messages that have been forwarded at least five times in WhatsApp, by double-tapping the magnifying glass icon to the right of the message. From there, your child can launch a Google search and decide for themselves whether the message was accurate or not. It's a good way to encourage young people to question things they see online.

Meet Our Expert

Parven Kaur is a social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience in the social media arena and is the founder of Kids N Clicks: a web resource that helps parents and children thrive in a digital world.

National Online Safety®
#WakeUpWednesday

SOURCES: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/#:~:text=As%20of%20March%202020%2C%20WhatsApp,U.S.%20dollars%20in%20February%202014, https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/, https://www.whatsapp.com/?lang=en, https://en.wikipedia.org/wiki/Indian_WhatsApp_lynchings, https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-update-latest-india-hoaxes-forward-messages-app-download-a8456011.html, https://www.bbc.co.uk/news/technology-52441007

What parents need to know about INSTAGRAM

AGE RESTRICTION 13+ Anyone over the age of 13 can create an account

Instagram is a hugely popular social networking app with over 1 billion users worldwide. The app, which is accessible on iOS and Android devices, allows users to upload images and videos to their feed, create interactive 'stories', exchange private messages or search, explore and follow other accounts they like. Images and videos can be transformed with an array of filters to edit the shot before sharing and anyone with an account can see others' online 'galleries' if their account is not private. To make posts easier to find, users can include searchable hashtags and captions to their uploads. That's why we've created this guide to help parents and carers understand exactly what Instagram is about.

HOOKED ON SCROLLING

Many social media platforms, Instagram included, have been designed in a way to keep us engaged on them for as long as possible. Behavioural economist, Nir Eyal, calls this the 'Hook Model' and the Instagram feed is a great example of this. Children and adults may find themselves scrolling to try and get a 'dopamine release'. Scrolling may become addictive and it can be difficult to stop until children find that 'something' they are looking for, quickly losing track of time as they get deeper into their Instagram feed.

SLIDING INTO DMS

Direct messages (or DMs) on Instagram allow users to share posts, images, videos, voice messages and calls between each other privately (or in a private group). Even if your child's account is set to private, anybody has the option to message them and send them content. If the person is not on your child's friends list, the message will still be sent to their inbox but the user has to accept their request to see the message.

INFLUENCER CULTURE

Influencers are sometimes paid thousands of pounds to promote a product, service, app and much more on social media. When celebrities or influencers post such an advert, they should add a disclaimer somewhere in the post which states that they have been paid for it. Commonly, this is well-hidden in the hashtags or in the comments of their post, making it unclear that their photo/video is actually an advert. This can be very misleading to young people who may be influenced into buying/wanting something promoted by somebody they admire, creating a false sense of reality and potentially affecting their mental health and wellbeing.

IMPACT ON WELLBEING

In a report by the RSPH, Instagram was ranked the worst for young people's mental health. Using filters on photos on Instagram can set unrealistic expectations and create feelings of inadequacy. Children may strive for more 'likes' by using realistically edited photos. Judging themselves against other users on the app might threaten their confidence or self-worth. In early 2019, Instagram banned images of self-harm and suicide, following the suicide of 14-year-old Molly Russell, who had reportedly been looking at such material on the platform. They since extended the ban to include drawings, cartoons and memes.

LIVE STREAMING TO STRANGERS

Live streaming on Instagram allows users to connect with friends and followers in real-time and comment on videos during broadcast. If your child's account is private, only their approved followers can see their story. It's important to note they may have accepted a friend request from someone they don't know, which means they could be live streaming to strangers. Children also risk sharing content they later regret, which could be re-shared online for years to come. Public accounts allow anybody to view, so we suggest your child blocks followers they don't know. In early 2019, data gathered by the NSPCC found that sex offenders were grooming children on Instagram more than on any other online platform.

IN-APP PAYMENTS

Instagram allows payments for products directly through the app. It operates under the same rules as Facebook Payments, which state that if you are under the age of 18, you can only use this feature with the involvement of a parent or guardian.

EXPOSING LOCATION

Public locations can be added to a user's photos/videos and also to their stories. While this may seem like a good idea at the time, it can expose the location of your child. This is particularly more of a risk if it is on their story, as it is real time. A photo which includes landmarks in the area, their school uniform, street name, house and even tagging in the location of the photo uploaded to Instagram can expose the child's location, making it easy to locate them. If their account is public, anyone can access their account and see their location.

HIJACKED HASHTAGS

Hashtags are an integral part of how Instagram works, but they can come with risks. One person may use a seemingly innocent hashtag with one particular thing in mind, and before you know it hundreds of people could be using the same hashtag for something inappropriate or dangerous that your child shouldn't be exposed to.

IGTV

Instagram TV (IGTV) works similar to YouTube. Users can watch videos from favourite accounts on the platform or create their own channel and post their own videos. It's important to note anyone can create an Instagram TV channel and doesn't have to be friends with a person to follow an account and watch their videos. In 2018 Instagram apologised and removed some of its TV content which featured sexually suggestive imagery of children. As the feature may encourage spending more time using the app, it's important to set time limits to avoid children's sleep or education being disturbed.

Top Tips for Parents & Carers

RESTRICT DIRECT MESSAGES

If your child receives a message from somebody they do not know, encourage them not to accept their message request and 'block' this person; this is the only way to stop them messaging your child again. Children can also 'tap and hold' the individual message to report it directly to Instagram as well as reporting the account itself.

LOOK OUT FOR #ADS

In 2019, the UK's Competition and Markets Authority launched an investigation into celebrities who were posting adverts on social media and not declaring that they were paid for. Influencers must clearly state that they have been paid for their posts, for example using a hashtag like #ad or #sponsored. Teach your child to look out for the signs of a paid post/advert and discuss with them that not everything they see from celebrities is their personal choice and opinion.

MANAGE NEGATIVE INTERACTIONS

If your child is receiving unwanted or negative comments, they can block that account so that they can't interact with them. This stops them seeing and commenting on their posts, stories and live broadcasts. In addition, your child can instantly delete unwanted comments from their posts, turn them off completely and control who can tag and mention them in comments, captions or stories, from everyone, only people they follow, or no one at all.

MANAGE DIGITAL WELLBEING

Instagram now has an in-built activity dashboard that allows users to monitor and control how much time they spend on the app. Users can add a 'daily reminder' to set a limit on how much time they want to spend on Instagram, prompting them to consider if its been too long. In addition, once users have caught up with all the previous posts since they last logged on, they'll receive a 'You've completely caught up' message. Both features can help you have a conversation with your child about how much time they are spending on the app and to set healthy time limits.

PROTECT PERSONAL INFORMATION

Your child may unknowingly give away personal information on their profile or in their live streams. Talk to them about what their personal information is and make sure that they do not disclose anything, including their location, to anyone during a livestream, comment, direct message or any other tool for communication on the platform, even to their friends.

USE A PRIVATE ACCOUNT

By default, any image or video your child uploads to Instagram is visible to anyone. A private account means that you have to approve a request if somebody wants to follow you and only people you approve will see your posts and videos. Children should also use a secure password and enable a two-factor authentication to add an extra layer of security to their account.

FILTER INAPPROPRIATE COMMENTS

Instagram has an 'anti-bullying' filter, which hides comments relating to a person's appearance or character, as well as threats to a person's wellbeing or health. The filter will also alert Instagram to repeated problems so that they can take action against the user if necessary. This is an automatic filter, which should always be enabled. Children can also report abusive behaviour or inappropriate/offensive material directly to Instagram from the app. This includes posts, comments and accounts.

TURN OFF SHARING

Even though this feature will not stop people from taking screenshots, it will stop others being able to directly share photos and videos from a story as a message to another user. This feature can be turned off in the settings. We also recommend turning off the feature which automatically shares photos and videos from a story to a Facebook account.

REMOVE PAYMENT METHODS

If you are happy for your child to have a card associated with their Instagram account, we suggest adding a PIN which needs to be entered before making a payment; this will also help prevent unauthorised purchases. This can be added in the payment settings tab.

DON'T FORGET TO BE VIGILANT & TALK TO YOUR CHILD ABOUT THEIR ONLINE ACTIVITIES!

Meet our expert

Parven Kaur is a social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience of working in the social media arena and is the founder of Kids N Clicks, a web resource helping parents and children thrive in a digital world.

NEW FOR 2020 INSTAGRAM REELS

Instagram Reels is the latest update from Instagram that gives users the ability to record and edit 15-second multi-clip videos with audio, effects, and new creative tools. It is the apps answer to TikTok and can be accessed via the Stories feature. Reels can be shared with friends and family, however, if your child has a public account, it could be shared wider via 'Explore' and viewed by millions of strangers online.

National Online Safety® #WakeUpWednesday

SOURCES:
https://about.instagram.com/about-us | https://about.instagram.com/community/safety | https://www.bbc.co.uk/news/uk-47410520

AGE RESTRICTION 13+

Twitter is a social networking site where users can post 'tweets' or short messages, photos and videos publicly. They can also share 'tweets' written by others to their followers. Twitter is popular with young people, as it allows them to interact with celebrities, stay up to date with news, trends and current social relevance.

What parents need to know about Twitter

TWITTER TROLLS

A 'troll' is somebody who deliberately posts negative or offensive comments online in a bid to provoke an individual for a reaction. Trolling, can include bullying, harassment, stalking, virtual mobbing and much more; it is very common on Twitter. The motive may be that the 'troll' wishes to promote an opinion or make people laugh, however, the pragmatics of what they post could be much more damaging, posting anything from racial, homophobic to sexist hate. Trolling can lead to devastating consequences for some victims.

INAPPROPRIATE CONTENT

Twitter gives users the opportunity and freedom to post their personal thoughts and opinions, meaning they can pretty much post anything they want despite restrictions on the platform. Swearing and inappropriate language is allowed if it does not violate the rules. If your child sees any inappropriate content, they might feel the need to replicate it at home or amongst their peers. Additionally, there are also a number of unofficial pornographic profiles on the platform that can easily be found and viewed without restrictions.

FAKE PROFILES

Fake Twitter accounts are made to impersonate a person, celebrity or public figure. As the accounts are not endorsed by the person they are pretending to be, they can often be used to scam or take advantage of young people who think that they're the real deal.

FAKE NEWS

The speed in which 'tweets' are shared on Twitter can be unbelievably fast, meaning that fake news can often be circulated across the platform very quickly. Fake news articles and posts can often be harmful and upsetting to young people and those associated with the fake news. In addition to this, it's very easy for people to quickly and unexpectedly retweet a tweet posted by your child, meaning there is no going back.

HIJACKED HASHTAGS

One of the most commonly used aspects of Twitter is the hashtag (#) – these allow users to easily search for specific trends, topics or subjects. However, due to the astronomical number of Twitter users, many hashtags can have 'different' intentions. One person may use a seemingly innocent hashtag, and before you know it, hundreds of people could be using the same hashtag for something inappropriate or dangerous that your child shouldn't be exposed to. This is common with 'trending' tweets, as people know that their tweet will be seen by a greater number of people.

MEMES NORMALISING RACISM, SEXISM AND HOMOPHOBIA

Twitter is a popular platform for sharing internet memes, helping to make concepts or ideas go viral across the internet. However, despite most meme's being innocent and harmless, some often include sexist, racist or homophobic messages. Although they are typically sent as a joke, this type of content is contributing to the normalisation of topics including racism, sexism and homophobia.

PROPAGANDA, EXTREMISM & RADICALISATION

Social media offers a continuous stream of real-time coverage of extremist activity. Twitter is one of the many platforms that is exploited by extremist groups to help promote violence, radicalise and recruit people to support their cause. These groups cleverly target vulnerable victims, often young people, and find a way to manipulate them into supporting their beliefs.

EVERYONE HAS ACCESS

Twitter has over 335 million monthly active users across all age groups. When a user signs up, tweets are public by default, meaning anyone can view and interact with posts instantly. Your child may change their mind about a tweet they have posted but even if they delete it, there's always a chance that someone can screenshot, retweet it or post it onto another platform.

Top Tips for Parents

CHECK ACCOUNT SETTINGS

We strongly advise that you thoroughly check your child's privacy settings. To take away some of the fear of your child's tweets being shared by anyone, you can always make their account protected. This means that anyone who wants to view what yout child has posted, it requires approval from them. In addition to this, you can change the settings so that they cannot receive 'direct' messages from anyone on the platform and that their location is not shared.

BLOCKING & REPORTING

If a particular account is causing your child trouble on Twitter, whether it's cyberbullying or upsetting content, you can simply block and report them. Blocking them will help to prevent them from viewing, messaging or following your child, and vice versa. Reporting an account will alert Twitter to investigate the profile.

MUTING ACCOUNTS

The 'mute' feature allows your child to remove an account's tweets from their timeline without unfollowing or blocking them. This means your child will stop getting notifications about a particular conversation but can still view it in their timeline. This can be useful if they are friends with someone but don't really like what they share. The other user will not know that they have been banned.

TWITTER TROLLS & THE LAW

From 2016, the CPS were able to exercise new laws that could see those who create "derogatory hashtags" or post "humiliating" photoshopped images jailed. They also announced the launch of a hate crime consultation, issuing a series of public policy statements centred on combating crimes against disabled people, as well as racial, religious, homophobic and transphobic hate crime. It's important your child knows about building a positive online reputation, as well as showing respect for others online and offline.

SENSITIVE CONTENT

By default, if Twitter has found a tweet that 'may contain sensitive content', Twitter will hide the content in the news feed and you will be shown a warning that states the content is sensitive. You then have the option to view it or not. This gives a chance for you to moderate potentially harmful images/videos before your child sees them. Unfortunately, some content may slip through the cracks and will be shown in the news feed. So, if you do see any sensitive content, you can report it. Twitter should then inspect the tweet and decide whether they deem it to be 'sensitive'.

MUTE HASHTAGS & PHRASES

Within the account settings, you have the ability to block certain words, hashtags or phrases from your child's timeline or notifications (e.g. swear words, inappropriate phrases, emojis, etc.)

TURN OFF VIDEO AUTOPLAY

'Autoplay' is a feature that automatically starts playing a new video seconds after another one ends on the platform. To avoid your child going from watching something innocent and harmless to something much more graphic or disturbing, you can turn this feature off in the settings and easily moderate the videos your child watches before they see them.

CONVERSATION & MONITORING

We always promote that you have regular open conversation with your child about their online activity, ensuring that they understand what healthy relationships are, what respect is, and how to be sensitive towards others' feelings. It's also important to monitor what they're doing online, including what they use the platform for, who they are talking to, and if they are viewing/taking part in anything that they shouldn't be. Discuss the dangers of the online world, such as fake news and online bullying - why do people involve themselves in these activities and what your child can do to prevent them.

TWITTER LISTS

Twitter lists allow your child to create other feeds besides the main timeline that only include certain accounts – this is a great way to segment followers based on common topics and interests.

SOURCES: Sources: https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts | https://help.twitter.com/en/safety-and-security/twitter-location-services-for-mobile | https://help.twitter.com/en/managingyour-account/two-factor-authentication | https://help.twitter.com/en/using-twitter/advanced-twitter-muteoptions | https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public | https://help.twitter.com/en/safety-and-security/public-and-protected-tweets | https://www.statista.com/statistics/493795/twitter-most-retweeted-posts/ | Smallbiztrends.com: 'What is Hashtag Hijacking?': https://smallbiztrends.com/2013/08/what-is-hashtag-hijacking-2.html
Christiededman.com: '5 things you should know about hashtags and your kids': http://christiededman.com/5-things-you-should-know-about-hashtags-your-kids/

YouTube

AGE RESTRICTION 13+

YouTube is an online platform - owned by Google - where anyone can upload & watch video content. All different types of information, advice & entertainment are uploaded & billions of people tune in to watch, rate & comment on it. As a parent, it's important you understand exactly what content your children might be seeing.

What parents need to know about YOUTUBE

INAPPROPRIATE CONTENT EASY TO ACCESS

Any child with a Gmail account can sign into YouTube & access videos. Some content is flagged 'age-restricted', but the platform relies on self-verification, meaning kids can get around the rules with a fake date of birth. This could enable access to vulgar, violent & dangerous videos.

USERS CAN PRIVATELY CONTACT YOUR CHILD

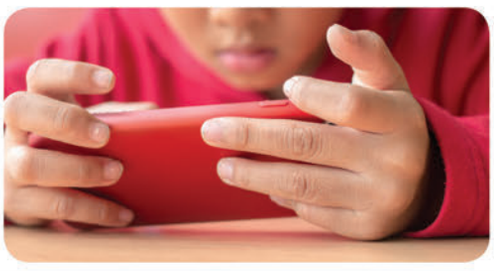
When your child is signed-in to YouTube with their Gmail account, there are various ways they can send & receive messages. This could be via the messages icon, or via the 'About' tab. There is scope here for users who your child does not know to make contact.

YOUTUBE SUGGESTS RELATED CONTENT

YouTube will often 'auto play' videos based on your child's viewing habits. The aim is to show related & appropriate content. But the problem is: it's possible your child will be exposed to inappropriate content that isn't accurately related.

'CHALLENGE VIDEOS' CAN GO TOO FAR

Challenge videos refer to a stunt you're encouraged to recreate & film. Many challenge videos can be harmless & for a good cause, like the Ice Bucket Challenge. But some are dangerous & even life threatening, such as the Bird Box Challenge.



SHARING VIDEOS RISKS YOUR CHILD'S PRIVACY

If your child has a Google account, they can upload their own videos. To do this, they must create a personal profile page known as a 'YouTube Channel'. The videos uploaded here can be viewed, commented on & shared by anyone. This could put your child's privacy at risk.

NOS National Online Safety®

#WakeUpWednesday

Meet our expert

Pete Badh is a writer with over 10+ years in research and analysis. Working within a specialist area for West Yorkshire Police, Pete has contributed work which has been pivotal in successfully winning high profile cases in court as well as writing as a subject matter expert for industry handbooks.

Tips To Protect Your Child

APPLY 'RESTRICTED MODE'

Restricted mode helps to hide any mature or unpleasant videos from your children. It uses YouTube's own automated system & looks at what other users flag as inappropriate content. It must be enabled in the settings menu on each individual device.

CHANGE WHO CAN SEE VIDEOS

You can change who can view your child's content in the settings. Options include Public (available to all), Private (only available to people you share it with & cannot be shared) or Unlisted (available to people you share it with & can be shared further).

BLOCK CONCERNING USERS

To help protect your child from cyber-bullies, harassment or persistent offensive comments, you can 'block' individual users. Doing so hides your child's videos from the user & stops the user being able contact your child in any way.

CUSTOMISE THEIR EXPERIENCE

Influence & control what your child watches using features such as Playlists (your videos play continuously rather than videos YouTube recommends) & Subscriptions (you choose channels your child can watch). It's also good to turn off auto play by toggling the blue button alongside the 'Up Next' title when viewing a video.

CREATE A 'FAMILY' GOOGLE ACCOUNT

Create a Google account to be used by the whole family. This will allow you to monitor exactly what your child is watching, uploading & sharing. Plus, your child's YouTube page will display their recently watched videos, searches, recommended videos & suggested channels.

GET YOUR OWN ACCOUNT

Create your own account so you can explore features yourself. Learn how to flag inappropriate videos, how to moderate comments & how to block users. This will help you feel more confident when providing advice & guidance to your children.

BE MINDFUL OF CYBERBULLYING

Once your child has posted a video, a worldwide audience can see it. Strangers may choose to comment on the video, both positively & negatively. So, be careful to check comments & any other interactions your child is making through the platform.

GET TO KNOW POPULAR CHANNELS

It's good to know which channels are most popular with your children. Some of the most popular channels right now are: PewDiePie, NigaHiga, Zoella, KSI, JennaMarbles, Markiplier, Smosh, ThatcherJoe & Casper Lee.

DON'T ASSUME YOUR CHILD IS TOO YOUNG

YouTube and YouTube Kids are quickly becoming the chosen viewing platforms for children between the ages of 3-15 & it's likely this trend will only increase. It's also possible children will become familiar with the platform at a younger & younger age. So it's important to understand the positives & negatives of the platform.

What Parents & Carers Need to Know about

SNAPCHAT

Age Rating 13+

Snapchat is a photo- and video-sharing app which also allows users to chat with friends via text or audio. Users can share images and videos with specific friends, or through a 'story' (documenting the previous 24 hours) visible to their entire friend list. Snapchat usage rose during the pandemic, with many young people utilising it to connect with their peers. The app continues to develop features to engage an even larger audience and emulate current trends, rivalling platforms such as TikTok and Instagram.

Connecting with Strangers

Even if your child only connects on the app with people they know, they may still receive friend requests from strangers. Snapchat's links with apps such as Wink and Hoop have increased this possibility. Accepting a request means that children are then disclosing personal information through the Story, SnapMap and Spotlight features. This could allow strangers to gain their trust for sinister purposes.

Inappropriate Content

Some videos and posts on Snapchat are not suitable for children. The hashtags used to organise content are determined by the poster, so an innocent search term could still yield age-inappropriate results. The app's Discover function lets users swipe through snippets of news stories and trending articles that often include adult content. There is currently no way to turn off this feature.

Compulsion and Excessive Use

Many users spend vast amounts of time trying to become a Snap Star. Snapchat is offering a share of $1 million, and the chance of online fame, to users who create and share the best videos. Children are therefore becoming obsessed with producing appealing content. The Spotlight feature's endless scroll of videos makes it easy for children to pass hours watching content, slowly getting addicted to the app.

Sexting

Sexting continues to be a risk associated with Snapchat. The app's 'disappearing messages' feature makes it easy for young people (teens in particular) to share explicit images on impulse. While these pictures *do* disappear – and the sender is notified if it has been screenshotted first – users have found alternative methods to save images, such as taking pictures with a separate device.

Damage to Confidence

Snapchat's signature filters and lenses are a popular way for users to enhance their 'selfie game'. Although many are designed to entertain or amuse, the 'beautify' filters on photos can set unrealistic body-image expectations and create feelings of inadequacy. Continually comparing themselves unfavourably against other Snapchat users could threaten a child's confidence or sense of self-worth.

Advice for Parents & Carers

Turn off Quick Add

The Quick Add feature helps people find each other on the app. This function works based on mutual friends or whether someone's number is in your child's contacts list. Explain to your child that this feature could potentially make their profile visible to strangers. We recommend that your child turns off Quick Add, which can be done in the settings (accessed via the cog icon).

Choose Good Connections

Snapchat has recently announced that it is rolling out a new safety feature: users will receive notifications reminding them of the importance of maintaining connections with people they actually know well, as opposed to strangers. This Friend Check up encourages users to delete connections with users they rarely communicate with to maintain their online safety and privacy.

Talk about Sexting

It may feel like an awkward conversation (and one that young people can be reluctant to have) but it is important to talk openly and non-judgementally about sexting. Discuss the legal implications of sending, receiving or sharing explicit images, as well as the possible emotional impact. Emphasise that your child should never feel pressured into sexting – and that if they receive unwanted explicit images, they should tell a trusted adult straight away.

Keep Profiles Private

Profiles are private by default, but children may want to make them public to gain more followers. You may wish to customise the settings so that your child's Stories can only be viewed by people they know well in real life. In SnapMaps, enabling 'Ghost Mode' (again via settings) prevents your child's location being seen; it also nullifies SnapMap 'status', which visibly displays a user's exact location for as long as they stay there.

Be Ready to Block and Report

If a stranger *does* connect with your child on Snapchat and begins to make them feel uncomfortable through bullying, pressure to send explicit images or by sending explicit images to them, your child can select the three dots on that person's profile and choose report or block. There are options to state why they are reporting that user (annoying or malicious messages, spam, or masquerading as someone else, for example).

Chat about Content

Talk to your child about what is and isn't wise to share on Snapchat (e.g. don't post explicit images or videos, or display identifiable details like their school uniform). Remind them that once something is online, the creator loses control over where it might end up, and who with. Additionally, Snapchat's 'Spotlight' feature has a #challenge like TikTok's: it's vital that your child understands the potentially harmful consequences of taking part in these challenges.

Meet Our Expert

Dr Claire Sutherland is an online safety consultant, educator and researcher who has developed and implemented anti-bullying and cyber safety policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviour of young people in the UK, USA and Australia.

National Online Safety®
#WakeUpWednesday

Sources: Status of Mind: Social media and young people's mental health | Life in Likes - Children's Commissioners Report | https://support.snapchat.com/en-US https://netsanity.net/snapchat-parent-review/ | BT.com | Independent.co.uk, https://mashable.com/article/snapchat-status-snap-maps/?europe=true, eSafety Commissioner, (2017), Young People and Sexting – Attitudes and Behaviours: Research Findings from the United Kingdom, New Zealand and Australia.

What Parents & Carers Need to Know about HOOP FOR

App Store Rating 13+

Hoop is a social networking app that syncs with Snapchat to help users build their community of friends. It works along similar principles to Tinder: swiping left or right will reject or accept potential contacts, making new connections in the process. When two users accept each other, they can then communicate via Snapchat. There is no chat function on Hoop itself: video and audio calls, messaging and image sharing all take place through Snapchat. When a user adds a new Hoop contact, they are essentially sharing their personal information from Snapchat.

No Age Verification

18+

The app groups ages 17–13 together and age children's profiles – and Hoop warns users that +18 years separately, so adults do not see they must input their real date of birth. However, there is no age verification system, meaning that an individual with intentions of grooming could sign up pretending to be a child, so that they could be connected with younger users.

In-app Purchases

Hoop offers in-app purchases that allow users to buy 'diamonds': the digital currency required to connect with others. Users can earn diamonds by watching videos, sharing links or contact lists, adding friends and completing surveys; alternatively, diamonds can be bought in packs, with costs ranging from 99p to 28.99£, which potentially could prove to be very expensive if a child has a payment method linked to their device.

Visible Location

Hoop gives users the option to share their Snap Story on their Hoop profile. Snap Stories are visible for 24 hours and, by default, show the user's exact location on the Snap Map. This means that not only will a young person's friends be able to see this information but all Hoop users too – including, potentially, individuals who may have sinister motives for pinpointing a child's whereabouts.

Grooming Risk

If a stranger uses Hoop to connect with your child on Snapchat, it means they would have access to your child's personal information, location, photos, videos and stories shared with their friends on Snapchat (unless your child has changed their privacy settings). Messages in Snapchat are automatically deleted after they're read, making it impossible for parents to monitor conversations.

Potential Compulsive Use

Users are rewarded with diamonds for hitting certain targets. To reach these milestones, young people may be inclined to add as many friends as possible – including strangers. Users are also assigned a level that is displayed on their Hoop profile; to achieve a higher level, users must add more connections – which provides an incentive for children to spend even more time on the app.

Possible Data Collection

One of the reasons Hoop has remained free to use is that it hosts video adverts and user surveys, which reward users with diamonds for taking part. This practice strongly suggests that the app collects personal information from the user, based on the adverts they watch and their responses to surveys, and then shares their data with third-party organisations.

Advice for Parents & Carers

Learn How to Report and Block

If your child sees or is sent something that makes them feel uncomfortable, Hoop has a reporting and blocking function. When reporting a user, you are asked to provide a reason why you are reporting them (for example, nudity or sexual content, hate speech, or using a fake age or gender). You then get a notification that the other user has been reported or blocked.

Limit Spending Power

If your child's device is linked to a bank card, a PayPal account or another form of payment, ensure that you have either removed this connection or adjusted the security settings, so that you get notifications of any attempts to make in-app purchases. Make sure that you have set a password which has to be entered for a purchase to go ahead.

Avoid Over-Sharing

Talk to your child about what they share online and who they share it with. Make them aware that once something is online, then anyone can see it. Talk to them about what might not be safe to post online (for example, things which could give away their home address or that of their school, explicit photos or their current location). Make sure that they don't share something they will regret later.

Be Wary of Strangers

Talk to your child about the dangers of connecting with strangers online. Encourage them not to engage in private messaging with people they don't know – particularly on Snapchat, as automatically disappearing messages makes the app difficult for trusted adults to monitor. Ask them to think about why they are adding all these connections and whether they genuinely need hundreds of 'friends' on Snapchat.

Adjust Privacy Settings

Check the privacy settings in place on your child's Snapchat account to make sure that only their friends or a custom group can see their stories, Snap Map and any images that they post. You may wish to seriously consider going into the settings and enabling 'ghost mode' to turn off the location services, so your child's whereabouts won't be publicly visible to other users.

Encourage Safe Communication

With the amount of time that young people spend communicating with others online, it's vital to ensure that these connections are positive and healthy ones. Regularly check which apps your child is using: if there are any new ones, talk to your child about what these apps are and how they work. If you are unsure about a new app, you could download it to try yourself and see if it is suitable.

Meet Our Expert

Dr Claire Sutherland is an online safety consultant, educator and researcher who has developed and implemented anti-bullying and cyber-safety policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviour of young people in the UK, USA and Australia.

National Online Safety®

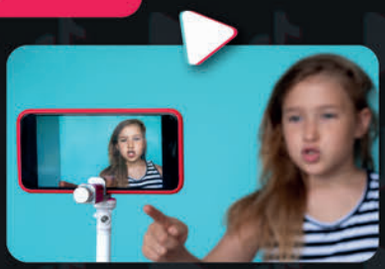
#WakeUpWednesday

SOURCES:

TikTok is a video-sharing social media app available on iOS and Android which lets users create, share, and view user created videos much in a similar manner to Facebook, Instagram and Snapchat. It's main draw, however, is that users can record and upload bite-sized looping videos of themselves lip-syncing and dancing to popular music or soundbites, often for comedic effect, which can then be further enhanced with filters, emojis and stickers. TikTok has been designed with the young user in mind and has a very addictive appeal. At the beginning of 2019 it skyrocketed in popularity to become the iOS store's most downloaded app with over 33 million downloads. Estimates suggest that it now has anything between 500 million and over 1billion monthly active users worldwide.

AGE RESTRICTION
12+
If under 18, supervision of a parent or legal guardian required.

What parents need to know about TIKTOK



MATURE CONTENT

On the iOS store, TikTok is listed as 12+. On the Google Play Store it is rated as 'Parental guidance recommended'. When signing up for the app, it's possible to lie about your age without any form of verification. As children scroll through their feed, most of the videos they're likely to come across are lighthearted or funny takes on dance routines which are designed to make people laugh. However there has been a slew of videos which have been reported for featuring drug and alcohol abuse, self-harm and sexual content, including young teens dressing overtly sexually and behaving suggestively. Given the deluge of material uploaded to TikTok every day, it's impossible to moderate everything and it can be quite common to come across explicit content on the 'for you' feed when logging into the platform.

INAPPROPRIATE MUSIC

TikTok revolves around creating music videos through lip-syncing and dancing. Inevitably, some of the music featured by users will contain explicit or suggestive lyrics. Given the undeniably young user base, there is a risk that children may look to imitate the explicit language they hear or the suggestive actions they see when viewing others user's videos on the app.

TIKTOK FAME

TikTok is very image focused and there is a notable preoccupation with appearing cool and attractive. Many teenagers now attempt to go viral and become what's known in-app as 'TikTok famous'. TikTok (and its predecessor musical.ly) has spawned its own celebrities – social media stars Loren Gray and Jacob Sartorious have been catapulted to fame through their initial exposure on the app. Obviously, most budding influencers looking to become the next big thing will be disappointed, but this may have the knock-on effect of making them go to more and more drastic lengths to get noticed.

ONLINE PREDATORS

As a social network, TikTok makes it easy to connect with other users. This includes the ability to comment on and react to other user's videos, follow their profile and download their content. Be aware that by default, any user can comment on your child's video if their account is set to public. Most interactions are harmless enough but as an app, TikTok is prone to predators because of the abundance of younger users.

ADDICTIVE NATURE

Social media is designed to be addictive and TikTok is no different. It can be fun and hugely entertaining. However, it is also because of this that it can be hard to put down. In addition to the short, punchy nature of the looping video format, the app's ability to keep you guessing what will come on screen next makes it easy to turn a five-minute visit into 45-minute visit.

IN-APP PURCHASES

Aside from the content, there's also the option to purchase in-app extras called 'TikTok coins'. Prices range from £0.99 for 100 coins to an eye-watering £93.99 for 10,000 coins. TikTok coins are used to purchase different emojis to reward content creators that a user finds funny or entertaining. In the iOS version of the app you can disable the option to buy TikTok coins but this sadly doesn't seem to be a feature in the Android version.

National Online Safety®
#WakeUpWednesday

Safety Tips For Parents

TALK ABOUT ONLINE DANGERS

Assuming your child is above the age limit to use the app, make sure you also take the time to talk to them about what they are seeing on the app. Have a dialogue, get them to give you their opinion on what is appropriate and model the correct behaviour for them. Go over why they shouldn't give out private information or identifiable photos and be positive and understanding of them. In the long run, getting them to think critically about what they're seeing goes a long way to keeping them social media savvy.

USE PRIVACY SETTINGS

Undoubtedly, the easiest way to safeguard your child on TikTok is to make sure their account is set to private. This means only those users your child approves can view, like, and follow their content. Setting the account to private may clash with your child's goal of social media superstardom, but it will keep their account secure from strangers. This setting can be enabled under the privacy and safety menu by pressing the ellipsis in the 'me' tab of the app. To be extra safe, there are additional controls available to toggle such as who can send comments and messages, among other options.

ENABLE RESTRICTED MODE

In the digital wellbeing section there's the ability to turn on restricted mode using a PIN. Restricted mode filters out content that is not age appropriate although it should be noted that this isn't always 100% fool proof. When enabling restricted mode, parents should still be vigilant to what their child is watching and take note that the algorithm moderating content is not infallible.

EXPLORE AND LEARN YOURSELF

Understanding and learning the app yourself is a great way to get to grips with TikTok. You could then even use the app with your child and watch some videos with them. If you are the parent of a teen, even if it does not make you popular, keep a close eye on what they're viewing and sharing. That said, it's a brilliant chance to turn it into a bonding opportunity with your child also. You could even unleash your inner performer and make videos with them while (more importantly) keeping them safe online.

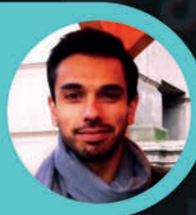
LEARN HOW TO REPORT AND BLOCK INAPPROPRIATE CONTENT

With the proper privacy settings in place, TikTok can be a safe space for your child to express themselves. However, just in case something does manage to slip through, make sure your child knows how to recognise and report content that isn't appropriate and get them to come to you about what they have seen. TikTok allows users to report offenders and comments within the app. You can also block individual users by going on their profile.

MODERATE SCREEN TIME

As entertaining as TikTok is, you can help your child moderate their time on the app by making use of the digital wellbeing section. Under the screen time management option, you can limit the daily allotted time allowed on the app in increments ranging from 40 to 120 minutes. You can also lock this preference behind a PIN number which has to be inputted in order to then exceed the daily time limit. This way your child can get their daily dose of memes without wasting away the day.

Meet our expert



Pete Badh is a writer with over 10+ years in research and analysis. Working within a specialist area for West Yorkshire Police, Pete has contributed work which has been pivotal in successfully winning high profile cases in court as well as writing as a subject matter expert for industry handbooks.

SOURCES:

ONLINE CONTENT

10 tips to keep your children safe online

The internet has transformed the ability to access content. Many apps that children use are dependent on user-generated content which can encourage freedom of expression, imagination and creativity. However, due to the sheer volume uploaded every day, it can be difficult for platforms to regulate and moderate everything, which means that disturbing or distressing images, videos or audio clips can slip through the net. That's why we've created this guide to provide parents and carers with some useful tips on keeping children safe online.

1 MONITOR VIEWING HABITS

Whilst most apps have moderation tools, inappropriate content can still slip through the net.

2 CHECK ONLINE CONTENT

Understand what's being shared or what seems to be 'trending' at the moment.

3 CHECK AGE-RATINGS

Make sure they are old enough to use the app and meet the recommended age-limit.

4 CHANGE PRIVACY SETTINGS

Make accounts private and set content filters and parental controls where possible.

5 SPEND TIME ON THE APP

Get used to how apps work, what content is available and what your child likes to watch.

6 LET CHILDREN KNOW YOU'RE THERE

Ensure they know that there is support and advice available to them if they need it.

7 ENCOURAGE CRITICAL THINKING

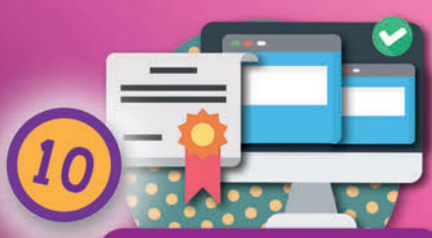
Talk about what people might post online and why some posts could cause distress.

8 LEARN HOW TO REPORT & BLOCK

Always make sure that children know how to use the reporting tools on social media apps.

9 KEEP AN OPEN DIALOGUE

If a child sees distressing material online; listen to their concerns, empathise and offer reassurance.



10 SEEK FURTHER SUPPORT

If a child has been affected by something they've seen online, seek support from your school's safeguarding lead.

National Online Safety®

#WakeUpWednesday

Your 24 Hour Free Helpline

03300 577 007

Completely discreet & non judgmental!

www.voicehelpline.co.uk

TSDESIGNS

UK Registered Charity: 1182874