Wath Academy

World-class learning	The highest expectations	No excuses	Growth mindset	Never give up	Everyone is valued	Integrity
World-class learning every lesson, every day	Everyone can be successful; always expect the highest standards	Create solutions not excuses; make positive thinking a habit	Believe you can improve; work hard and value feedback	Resilience is essential; be relentless in the pursuit of excellence	Diversity is celebrated; see the best in everyone	Be trustworthy and honest; deliver on promises and walk the talk

Parent E-Safety Guidance

UK Safer Internet Centre

As a parent or carer you play a key role in helping your child to stay safe online. You don't need to be an expert on the internet to help keep your child stay safe online. Our advice and resources are here to support you as you support your child to use the internet safely, responsibility and positively.

Using artificial intelligence

As more children and young people use artificial intelligence (AI) for schoolwork, advice and companionship, they'll need support on using tools safely. Explore this collection of resources to help you support age-appropriate use and keep children safer.

SEND digital safety advice for parents and carers.

This guide helps parents to support young people with Special Educational Need and Disabilities. To help ensure that their time spent online is positive and safe.

Online home filtering controls

Step by step instructions to set controls on major broadband providers and mobile networks. Broadband, mobile and WiFi providers offer filters to limit the inappropriate content eg, gambling, pornography, violence. These filters normally require manual set up, these guides are here to help and offer videos and visual instructions to help ensure you are able to put all the right protection in place to allow your children safer access to the internet at home.

Wath Academy – E-Safety Parents Evening

Useful links

Internet Matters – My Family's Digital Toolkit.

Answer some simple questions about your children's digital habits **(takes just a few minutes)**
Provide an email address to receive your own personalised online safety toolkit

Use the toolkit to:
Get age-specific advice to support your children online
Learn about popular apps and platforms your children use
Get information about how to deal with any online safety concerns
Get recommendations for digital tools to support their interests and wellbeing

Internet Matters – Get kids tech set up safe

Offers help on how to set up multiple devices from smart speakers to educational toys.

Internet Matters – Reporting issues

This link will take you directly to the report pages of organisations who can offer advice.There are also links to online issue advice pages,where you can find advice on specific issues + recommended forums to get support and talk to other parents.

Internet Matters – Social media advice

Provides advice on managing fake news, excessive screen time, scams & hacking, online spending + lots more

NSPCC – Resources for children with SEND

NSPCC have partnered with Ambitious about Autism to create online safety tips, advice and activities for parents and carers of children with SEND, including children with dyslexia, autism and speech and language difficulties.

What Schools Need to Know about THE ONLINE SAFETY ACT

The Online Safety Act was passed into UK law in October 2023, with the aim of establishing major new layers of protection for children when they're online. The government has pledged "a zero-tolerance approach to protecting children from online harm" – and the act certainly includes more powerful legislation which should help to safeguard young people in the digital world. Our guide summarises the key points for schools ...

WHAT THE ACT WILL DO

HARMFUL CONTENT

Social media sites must rapidly remove illegal and/or harmful content such as bullying or harassing comments; pornography; and content that supports extremist activity or encourages or depicts violence, suicide, self harm or eating disorders. If they fail to do so, they can be fined up to 10% of their global revenue while their executives may even face jail time.

ANIMAL CRUELTY

Content featuring cruelty to animals is now prohibited, even if it originates from abroad (where the law may be different). Again, it is the platform's responsibility to remove this.

MORE TRANSPARENCY

Sites must be transparent about the hazards that any children using them could encounter – by publishing risk assessments for their platforms, for instance.

HOSTING MISLEADING ADVERTS

Scams and fraudulent adverts must be blocked or removed, or the hosting companies are liable to be fined.

NON-CONSENSUAL SHARING

It's now easier to convict online abusers or people who share intimate images without consent, while legislation on the criminality of deepfakes has been clarified. The new laws also relate to any individuals who even *threaten* to share such images. This should help to protect women and girls in particular online.

REPORTING AND FILTERING

Sites should have easy reporting mechanisms for children (or their parents and carers) to flag up problems quickly. They must also provide options to filter out unwanted content.

AGE-RESTRICTED MATERIAL

Sites must prevent children from accessing age-inappropriate material. This includes enforcing age limits and implementing robust age verification.

What this means for you

The act has some specific implications for schools: it's essential that leaders understand the new legislation's scope and limitations. The act is certainly a positive step, but as artificial intelligence and other advances in tech continue to produce new challenges, schools will still need to remain extremely vigilant.

KNOW WHERE TO GET HELP

Look out for the Code of Conduct that Ofcom is creating in response to the Online Safety Act. Note that the new legislation doesn't mean an instant change: many of its elements will only come into force at the end of 2023. An Ofcom consultation on 'protecting people from illegal harms online' will be running until February 2024.

REMEMBER THE ESSENTIALS

Remain mindful of your organisation's own online activities: the legal duty for schools to maintain appropriate software monitoring and filtering, for example, will not change.

WATCH FOR FUTURE DEVELOPMENTS

There are some issues on which the legislation remains less clear for now: whether it's possible for Ofcom to scan encrypted private messages (such as on WhatsApp) has yet to be resolved, for instance – making this an area where, for the moment, young people have less legal protection.

UNDERSTAND AND EXPLAIN

Staff should learn how to raise concerns with tech companies whose platforms contain anything upsetting or unpleasant. Students also need to be made aware of the newly strengthened laws relating to cyber-bullying, sexting or posting inappropriate content. Young people *do* make mistakes online – so the clearer their understanding of the possible consequences, the better.

ENGAGE WITH PARENTS

Schools should also explain to parents and carers the new possibilities that the Online Safety Act affords them in terms of protecting their children. Many parents may have previously felt that there was little they could do about changing online platforms' content; they now have a far greater level of support when complaining about a company or the behaviour of an individual.

Meet Our Expert

Luke Ramsden is Senior Deputy Headmaster and Director of Safeguarding for the St Benedict's family of schools. He is a regular speaker at conferences and writes in the TES (among other journals) on school leadership, pastoral care and safeguarding. In 2022, he was named Pastoral Leader of the Year at the National Awards for Pastoral Care in Education.

10 Top Tips for Parents and Educators

SUPPORTING SAFE USE OF AI

Artificial Intelligence (AI) is increasingly woven into young people's digital lives. It can offer some educational benefits and day-to-day assistance; however, it also raises concerns about misinformation, privacy, fairness, and safety. This guide provides parents and educators with practical strategies to support young people to navigate AI tools responsibly, and to use them safely and with discernment.

1 DEMYSTIFY WHAT AI REALLY IS

Children encounter AI in most online places, including games, streaming platforms, and school tools. Explain that AI uses patterns from past data to make decisions, but it doesn't think or feel like humans. Use age-appropriate examples, like how recommendations on YouTube or Netflix work, to build understanding and prevent false beliefs about AI being all-knowing or alive.

2 TALK ABOUT RISKS OF MISINFORMATION

AI can create convincing false information, including deepfake videos, photos, and fake 'facts'. Encourage children to think critically about what they see and read. Teach them to double-check information using reliable sources, to look at images and videos carefully, and to ask an adult if something doesn't seem right.

3 DISCUSS DATA AND PRIVACY

Explain that AI systems learn by analysing lots of data, sometimes including personal information. Help young people to be mindful of what they share online and why protecting personal data matters. Model good habits like reading app permissions together or reviewing what's collected by voice assistants like Alexa or Siri.

4 ENCOURAGE CREATIVE USE OF AI

Support children, when using AI tools, to explore ideas, make art, or build projects. This fosters confidence, imagination, and independent thinking. When children use AI creatively, rather than just passively consuming it, they are more likely to stay engaged and make thoughtful choices.

5 USE AGE-APPROPRIATE AI TOOLS

Not all AI platforms are suitable for children. Choose tools designed for education or creativity, with clear safety policies. Review terms of use and privacy settings, and help children use them in age-appropriate ways. For example, some chatbot tools mimic conversation but should only be used with guidance and boundaries in place.

6 USE AI TOGETHER

Exploring AI tools together can help adults understand how they work and spot potential issues. Try co-writing a story with an AI writing assistant or experimenting with an AI art tool. This encourages curiosity, helps you stay informed about the latest AI tools, and allows you to reinforce safe and respectful use while modelling critical thinking.

7 SET BOUNDARIES FOR AI USE

Establish when, where, and how AI tools can be used, just as you would with any digital technology. For example, you might agree not to use AI tools to complete school assignments without permission, or to avoid unsupervised use of voice assistants. Consistent boundaries help manage overuse and misuse.

8 WATCH FOR OVERRELIANCE

Some AI tools, like homework help apps, may be tempting shortcuts. Encourage children to use AI to support their thinking, not replace it. Celebrate effort and process over perfect answers. Reinforce that mistakes are part of learning and that relying too heavily on AI can limit real understanding.

9 TEACH DIGITAL ETHICS AND LITERACY

Help children explore how AI works, where it might be biased, and why ethical thinking matters. Building digital literacy alongside ethical awareness ensures children engage with AI critically, not just conveniently. Help young people to understand that not all people use AI for legitimate purposes; some use it for malicious reasons. Encourage questions about fairness, representation, and who benefits from certain tools; talk about algorithms, echo chambers, and the impact of automation on daily life.

10 STAY CURIOUS AND INVOLVED

AI is developing rapidly, and staying informed helps you support the young people in your care. Follow trusted sources for updates and keep the conversation going. If a child brings up a new AI trend or tool, take the opportunity to learn about it together. Showing interest builds trust and strengthens digital resilience.

Meet Our Expert

Home to the world's largest CPD library for educators, The National College has transformed the way education establishments go about developing their workforces and managing compliance. Our three memberships help all phases and types of setting raise standards, save time, reduce risk, and build a culture of improvement.

#WakeUpWednesday®

The National College®

@wake_up_weds /www.thenationalcollege @wake.up.wednesday @wake.up.weds

What Parents & Carers Need to Know about X

AGE RESTRICTION 13+

In October 2022, the enormously popular social media network Twitter was purchased by tech tycoon Elon Musk. That sparked a host of changes to the platform – not all which have been received positively by its fans. The alterations have continued with each passing month, many of them raising online safety concerns among the 530 million users of Twitter (now rebranded as simply X). With further adjustments reportedly in the pipeline, X has attracted more than its usual share of controversy and caution in recent times.

WHAT ARE THE RISKS?

A BLOCK ON BLOCKING

X has announced plans to remove its blocking feature. Previously, this stopped other users from viewing your profile or sending you direct messages, while also hiding their posts from your feed. Only this latter function will now remain. The decision has been criticised by some members, who feel that blocking (in its current form) protects them from X users who 'promote denial and hatred'.

AGE-INAPPROPRIATE CONTENT

CENSORED

Many of X's less age-appropriate posts can feature anything from extreme political views to pornography. While accounts marked as 18+ are restricted from non-members, it's still fairly easy to stumble across this material accidentally. X's new 'For You' page also shows content from accounts that a user *doesn't* already follow – meaning that almost anything could end up on a child's feed.

LIMITED REPORTING FEATURES

X offers a premium membership, with some functionality (such as controlling who can view and reply to your posts) increasingly being made exclusive to those who pay the subscription fee. Several commentators have speculated that X could one day become an exclusively paid-for service, with access to accounts being revoked for anyone unwilling or unable to take out a subscription.

VERIFICATION FOR SALE

Historically, Twitter's moderators granted account verification: certifying someone as authentic by placing a blue tick next to their username. One of X's earliest changes was to place verification behind a paywall; this caused the number of celebrity impersonators to rise and left no way to distinguish, say, a legitimate influencer from a copycat fake account seeking to exploit other users.

Advice for Parents & Carers

PROTECT PRIVACY

Unsavoury characters may try to gain access to a young person's X account – either to view their posts and gather information on them, or to completely take control of it. To minimise risk, ensure the account has a strong password and enable the 'Protect Your Posts' feature (via the account settings), so that strangers can't view your child's posts without first being approved as a follower.

DON'T RISE TO THE BAIT

To gain more views and followers, some X users post deliberately inflammatory comments on sensitive topics such as race, sexual orientation and gender issues. Many young people could find this upsetting. Emphasise that, if your child encounters someone spreading hate on X, it's best not to give that person what they want: an argument. Ignore them, mute their account and move on.

STAY ALERT FOR IMPOSTERS

Make sure your child understands that X's blue ticks no longer guarantee the identity of anyone on the platform. While it might be exciting if a celebrity liked your child's post, it could just as easily be an imposter with malicious intentions. If your child's not 100% sure that an X user actually *is* who they claim to be, advise them to err on the side of caution and avoid interacting with that account.

ONLY FOLLOW TRUSTED ACCOUNTS

Using the 'Following' tab on X helps to ensure that the only content your child sees has come from accounts they've chosen to follow: this should reduce the chance of them inadvertently being exposed to harmful, violent or explicit content. Show your child how to report another user's account if, say, they're behaving inappropriately by spreading misinformation or offensive opinions.

BE READY TO TAKE ACTION

If your child suffers harassment on the platform or becomes the target of a hack, you could consider deactivating their account entirely. Recently, X's safety features have been criticised for allegedly failing to protect users' wellbeing – so if your child is being subjected to abusive messages or similar mistreatment on the platform, it might be prudent to remove them from X altogether.

Meet Our Expert

Lloyd Coombes is Editor-in-Chief of gaming and esports site GGRecon and has worked in the gaming media for around four years. Always eager to test out the latest apps, games and online trends, he's also a parent who understands the importance of online safety. Writing mainly about tech and fitness, his articles have been published on influential sites including IGN and TechRadar.

National Online Safety
#WakeUpWednesday

12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

As a society, we're increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off; streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops ... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It's essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS 'CYBER RESILIENCE?'

Cyber resilience focuses on three key areas: reducing the likelihood of a cyber attack gaining access to our accounts, devices or data; reducing the potential impact of a cyber incident; and making the recovery from a cyber attack easier, should we ever fall victim to one.

1. PASSWORDS: LONGER AND LESS PREDICTABLE

The longer, less common and predictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre's 'three random words' guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS

When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you've signed up for. If cyber criminals gain access your username and password for one site or service, they'll definitely try them on others.

3. USE A PASSWORD MANAGER

A good way to juggle different passwords for every site or service you use is to have a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, 1Password and Keeper are all excellent password managers.

4. BACK UP YOUR DATA

Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it's extremely important or sensitive information, you could even decide to keep more than one back-up version – by saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they do manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY

Some services let you set 'recovery questions' – such as your birthplace or a pet's name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals' task far harder.

7. SET UP SECONDARY ACCOUNTS

Some services provide the facility to add secondary accounts, phone numbers and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you're having trouble logging in or if you're trying to take back control of your account after a cyber attack.

8. KEEP HAVING FUN WITH TECH

Consider our tips in relation to the gadgets and online services your household uses. Protect yourself and your family, and don't let the bad guys win: devices are not only integral to modern life but also a lot of fun – so as long as you keep safety and security in mind, don't stop enjoying your tech.

9. CHECK FOR BREACHES

You can check if your personal information has been involved in any known data breaches by entering your email address at www.haveibeenpwned.com (yes, that spelling is correct). It's useful if you're worried about a possible attack – or simply as motivation to review your account security.

10. CHANGE DEFAULT IOT PASSWORDS

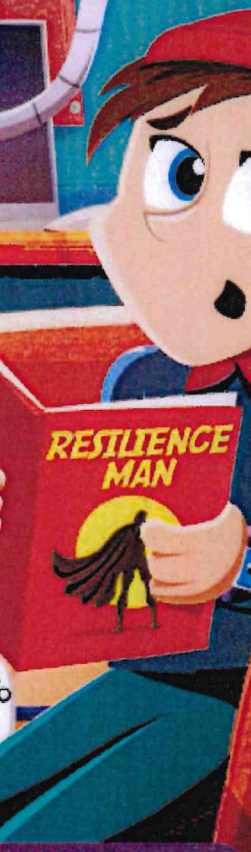
Devices from the 'Internet of Things' (IoT), such as 'smart' home appliances, are often supplied with default passwords. This makes them quicker to set up, but also less secure – criminals can identify these standard passwords more easily, so change them on your IoT devices as soon as possible.

11. KEEP HOME DEVICES UPDATED

Download official software updates for your household's mobile phones, laptops, consoles and other internet-enabled devices regularly. Security improvements and fixes are a key feature of these updates – so by ensuring each device is running the latest version, you're making them more secure.

12. STAY SCEPTICAL

Cyber criminals commonly use various methods, including emails, text messages and social media posts. Be cautious of any messages or posts that are out of the ordinary, offer something too good to be true or emphasise urgency – even if they appear to come from someone you know.



Meet Our Expert

Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.

Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words | https://haveibeenpwned.com

National Online Safety® #WakeUpWednesday

Tips for Encouraging Open Discussions about DIGITAL LIVES

The online world is an entirely familiar and commonplace part of life for today's children and young people, far more so than for previous generations. There are many positives to children being able to access online materials, so it's important not to demonise the internet, games and apps, and limit the benefit of their positive aspects. At the same time, we do have a responsibility to educate children about the hazards they may encounter online (just as we would about real-world dangers) so it's essential that we don't shy away from talking to them about the complex – and often sensitive – subject of what they do and what they see when they're online.

Here are some suggestions for kicking off conversations with your child about their digital life ...

MAKE YOUR INTEREST CLEAR

Showing enthusiasm when you broach the subject signals to your child that you're keen to learn about the positives of their online world. Most children enjoy educating adults and will happily chat about what they use the internet for, or what games and apps they're into and how these work. Asking to see their favourite games and apps in action could help you spot any aspects that may need your attention – such as chat functions which might require a settings adjustment to limit contact with strangers. Keep listening even if your child pauses for a long time: they could be considering how to phrase something specific, or they may be gauging your reaction.

BE OPEN AND HONEST, APPROPRIATE TO THEIR AGE

At various stages, children and young people become curious about puberty and how their body changes; about relationships; about how babies are made; and about sexual health. If your child knows that they can discuss these sensitive subjects with you, they tend to be less likely to go looking online for answers – which can often provide them with misleading information and, in some cases, lead to them consuming harmful content. Don't worry if you don't immediately know the answers to their questions – just find out for yourself and go back to them once you have the facts.

REMIND YOUR CHILD THEY CAN ALWAYS TALK TO YOU

In my role I work with many children and young people who admit being reluctant to tell a trusted adult about harmful content they've viewed online, in case it leads to having their devices confiscated. Emphasise to your child that you're always there to listen and help; reassure them that if they do view harmful content, then they are not to blame – but talking about it openly will help. Children shouldn't be expected to be resilient against abuse or feel that it's their job to prevent it.

DISCUSS THAT NOT EVERYTHING WE SEE ONLINE IS REAL

Here, you could give examples from your own digital life of the online world versus reality – for example, those Instagram posts which show the perfect house: spotlessly clean, never messy and immaculately decorated. Explain to your child that there are many other aspects of the online world which are also deliberately presented in an unrealistic way for effect – such as someone's relationship, their body, having perfect skin and so on.

TRY TO REMAIN CALM

As much as possible, try to stay calm even if your child tells you about an online experience that makes you feel angry or fearful. Our immediate emotions frequently influence the way we talk, so it's possible that your initial reaction as a parent or carer could deter a child from speaking openly about what they've seen. Give yourself time to consider the right approach, and perhaps speak with other family members or school staff while you are considering your next steps.

CREATE A 'FAMILY AGREEMENT'

Involving your whole household in coming up with a family agreement about device use can be immensely beneficial. You could discuss when (and for how long) it's OK to use phones, tablets, consoles and so on at home; what parental controls are for and why they're important; and why it's good to talk to each other about things we've seen or experienced online (both good and bad). Explaining your reasoning will help children to understand that, as trusted adults, we want to make sure they are well informed and kept safe. Allowing children to have their say when coming up with your family agreement also makes them far more likely to stick to it in the long term.

KEEP TALKING!

The most valuable advice we can give is to keep talking with your child about their digital lives. You could try using everyday situations to ask questions about their online experiences.

Meet Our Expert

Rebecca Jennings of RAISE (Raising Awareness in Sex Education) has almost 20 years' experience delivering relationships and sex education and training to schools, colleges and other education providers. A published author on the subject, she also advises the Department of Education on the staff-training element of the RSHE curriculum.

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about TIKTOK

AGE RESTRICTION 13+

TikTok is a video-sharing social media app which lets people create, view and download looping 15-second clips. Typically, these are videos of users lip-syncing and dancing to popular songs or soundbites (often for comic purposes), enhanced with filters, effects and text. Designed with young people in mind, TikTok skyrocketed in popularity in 2019 and has featured near the top of download charts ever since. It now has around a billion users worldwide.

AGE-INAPPROPRIATE CONTENT

Most videos appearing on a child's feed are light-hearted and amusing. However, some clips have been reported for featuring drug and alcohol abuse, themes of suicide and self-harm, or young teens acting in a sexually suggestive way. The sheer volume of uploads is impossible to moderate entirely – and since TikTok Jump's introduction in mid-2021, users can view third-party content outside the app.

18 CENSORED

EXPLICIT SONGS

W&#*!

TikTok primarily revolves around videos of users lip-syncing and dancing to music. Inevitably, some featured songs will contain explicit or suggestive lyrics. Given the app's young user-base, there is a risk that children may view older users' videos and then be inclined to imitate any explicit language or suggestive actions.

TIKTOK FAME

OSCAR♡

The app has created its own celebrities: Charli D'Amelio and Lil Nas X, for example, were catapulted to fame by exposure on TikTok – leading to many more teens attempting to go viral and become "TikTok famous". While most aspiring stars hoping to be 'the next big thing' will find it difficult, setbacks may in turn prompt them to go to even more drastic lengths to get noticed.

HAZARDOUS VISIBILITY

Connecting with others is simple on TikTok – including commenting on and reacting to users' videos, following their profile and downloading their content. The majority of these interactions are harmless, but – because of its abundance of teen users – TikTok *has* experienced problems with predators contacting young people.

ADDICTIVE NATURE

Like all social media, TikTok is designed to be addictive. It can be hugely entertaining – but that also makes it hard to put down. As well as the punchy nature of the short video format, the app's ability to keep users intrigued about what's coming next mean it's easy for a 5-minute visit to turn into a 45-minute stay.

IN-APP SPENDING

There's an in-app option to purchase 'TikTok coins', which are then converted into digital rewards for sending to content creators that a user likes. Prices range from 99p to an eye-watering £99 bundle. TikTok is also connected with Shopify, which allows users to buy products through the app.

Advice for Parents & Carers

TALK ABOUT ONLINE CONTENT

Assuming your child is above TikTok's age limit, talk to them about what they've viewed on the app. Ask their opinion on what's appropriate and what isn't. Explain why they shouldn't give out personal details or upload videos which reveal information like their school or home address. In the long run, teaching them to think critically about what they see on TikTok could help them to become social-media savvy.

MAINTAIN PRIVACY SETTINGS

The default setting for all under 16s' accounts to 'private'. Keeping it that way is the safest solution: it means only users who your child approves can watch their videos. The 'Stitch' (which lets users splice clips from other people's videos into their own) and 'Duet' (where you build on another user's content by recording your own video alongside their original) features are now only available to over 16s. This might clash with your child's ambitions of social media stardom, but it will fortify their account against predators.

LEARN ABOUT REPORTING AND BLOCKING

With the correct privacy settings applied, TikTok is a relatively safe space. However, in case something *does* slip through, make sure your child knows how to recognise and report inappropriate content and get them to come to you about anything upsetting that they've seen. TikTok allows users to report anyone breaching its guidelines, while you can also block individual users through their profile.

ENABLE FAMILY PAIRING

'Family Pairing' lets parents and carers link their own TikTok account to their child's. Through your mobile, you can control your child's safety settings remotely – including limiting screen time, managing their ability to exchange messages (and with whom) and blocking a lot of age-inappropriate content. TikTok's Safety Centre also provides resources for parents and carers to support online safety among families. These resources can be found on their website.

USE RESTRICTED MODE

In the app's 'Digital Wellbeing' section, you can filter out inappropriate content (specific content creators or hashtags, for instance) using 'Restricted Mode'. This can then be locked with a PIN. You should note, though, that the algorithm moderating content isn't totally dependable – so it's wise to stay aware of what your child is watching.

MODERATE SCREEN TIME

As entertaining as TikTok is, you can help your child to manage their time on it in the 'Digital Wellbeing' section. Under 'Screen Time Management', you can limit the daily permitted time on the app (in increments ranging from 40 minutes to two hours). This preference can also be locked behind a PIN. That way, your child can get their regular dose of TikTok without wasting the whole day.

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.

SOURCES TikTok.com

National Online Safety® #WakeUpWednesday

What Parents & Carers Need to Know about INSTAGRAM

follow

WHAT ARE THE RISKS?

like

AGE RATING 13+

Instagram is one of the most popular social media platforms in the world, with over 1 billion users worldwide. The platform allows users to upload images and videos to their feed, create interactive 'stories', share live videos, exchange private messages or search, explore and follow other accounts they like – whilst at the same time continuously updating and adding new features to meet the needs of its users.

ADDICTION

Many social media platforms are designed in a way to keep us engaged on them for as long as possible. There's a desire to scroll often/more in case we've missed something important or a fear of missing out. Instagram is no different and young people can easily lose track of time by aimlessly scrolling and watching videos posted by friends, acquaintances, influencers or even strangers.

PRODUCT TAGGING

Product tags allow users (particularly influencers who are sponsored to advertise products) to tag a product or business in their post. This tag takes viewers, regardless of age, directly to the product detail page on the shop where the item can be purchased and where children may be encouraged by influencers to purchase products they don't necessarily need.

EXCLUSION AND OSTRACISM

Young people are highly sensitive to ostracism. Feeling excluded can come in many forms such as: not receiving many 'likes', not being tagged, being unfriended, having a photo untagged, or not receiving a comment or reply to a message. Being excluded online hurts just as much as being excluded offline – with children potentially suffering lower moods, lower self-esteem, feeling as if they don't belong or undervalued.

PUBLIC ACCOUNTS

Product tagging on Instagram only works on public accounts. If your child wants to share their clothing style, make-up etc and tag items in a post then they may be tempted to change their settings to public, which can leave their profile visible to strangers.

Buy Milk

GOING LIVE

Live streaming on Instagram allows users to connect with friends and followers in real-time and comment on videos during broadcast. Risks increase if the account is public because anyone can watch and comment on their videos, including strangers. However, other risks include acting in ways they wouldn't normally or being exposed to inappropriate content or offensive language.

INFLUENCER CULTURE

Influencers can be paid thousands of pounds to promote a product, service, app and much more on social media – the posts can often be identified because they state they're a 'paid partnership'. Ofcom found that young people often attempt to copy-cat influencer behaviour for their own posts to gain likes, sometimes posting content which may not be age-appropriate.

UNREALISTIC IDEALS

Children compare themselves to what they see online in terms of how they look, dress, their body shape, or the experiences others are having. The constant scrolling and comparison of unrealistic ideals can lead to children feeling insecure about their own appearance, questioning how exciting their own lives are and having a fear of missing out.

Advice for Parents & Carers

HAVE OPEN DIALOGUE

Talk to your child about live videos and the risks involved and how they can do it safely with family and friends. Talk to them about ensuring they have safety settings on so only followers can view them live, and maybe help them prepare what they would say when they do go live.

REMOVE PAYMENT METHODS

If you're 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 can be added in the payment settings tab and will also help prevent unauthorised purchases.

USE MODERATORS

Instagram has launched 'live moderators' on Instagram live where creators can assign a moderator and give them the power to report comments, remove viewers and turn off comments for a viewer. It's recommended to keep devices in common spaces so that you are aware if they do go live or watch live streaming.

FAMILIARISE YOURSELF

Instagram is one social media app which has its safety features available to parents in a user-friendly manner. The document provides examples of conversation starters, managing privacy, managing comments, blocking and restricting and can be found on the Instagram website>community>parents.

FOLLOW INFLUENCERS

Following influencers will allow you to monitor what they're sharing as well as being able to discuss anything which you deem inappropriate. Talk to your child about who they follow and help them develop critical thinking skills about what the influencer is trying to do. For example, are they trying to sell a product by promoting it?

BE VIGILANT AND REASSURE

Talk to your child about the use of filters. While they can be fun to use they don't represent the real them. If you find your child continuously using a filter, ask them why and reassure them that they are beautiful without it to build up their feelings of self-worth. Discuss the fact that many images online are filtered and not everyone looks 'picture perfect' in real life, which can also lend itself to discuss what is real and not real online.

MANAGE LIKE COUNTS

Due to the impact on mental wellbeing, Instagram has allowed users to change the focus of their experiences online away from how many likes a post has by hiding the like counts. Users can hide like counts on all the posts in their feed as well as hiding the like counts on their own posts. This means others can't see how many likes you get. This can be done by going into settings > notifications > posts > likes > off

BALANCE YOUR TIME

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 it's been too long with a 'take a break' message. There's also the option to mute notifications for a period of time. These 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.

Meet Our Expert

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

Sources: https://about.instagram.com/blog/announcements/introducing-family-center-and-supervision-tools | https://about.instagram.com/en_US/blog/introducing-live-and-shop-tab

National Online Safety® #WakeUpWednesday

What Parents & Carers Need to Know about SNAPCHAT

AGE RESTRICTION 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 predators to gain their trust for sinister purposes.

EXCESSIVE USE

There are many features that are attractive to users and keep them excited about the app. Snap streaks encourage users to send snaps daily, Spotlight Challenges give users to the chance to obtain money and online fame, and the Spotlight feature's scroll of videos makes it easy for children to spend hours watching content.

INAPPROPRIATE CONTENT

Some videos and posts on Snapchat are not suitable for children. The hashtags used to group 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.

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 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. Comparing themselves unfavourably against other Snapchat users could threaten a child's confidence or sense of self-worth.

VISIBLE LOCATION

My Places lets users check in and search for popular spots nearby – such as restaurants, parks or shopping centres – and recommend them to their friends. The potential issue with a young person consistently checking into locations on Snapchat is that it allows other users in their friends list (even people they have only ever met online) to see where they currently are and where they regularly go.

Advice for Parents & Carers

TURN OFF QUICK ADD

The Quick Add function 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.

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.

KEEP ACCOUNTS PRIVATE

Profiles are private by default, but children may make them public to gain more followers. Your child can send Snaps directly to friends, but Stories are visible to everyone they have added, unless they change the settings. If they use SnapMaps, their location is visible unless 'Ghost Mode' is enabled (again via settings). It's prudent to emphasise the importance of not adding people they don't know in real life. This is particularly important with the addition of My Places, which allows other Snapchatters to see the places your child regularly visits and checks in. Additionally, it's important to be cautious about Shared Stories as this allows people who are not on your contact list access to the post.

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).

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.

NOS National Online Safety®
#WakeUpWednesday

Sources: State of Mind: Social media and young people's mental health | Life in Likes – Children's Commissioner Report | https://support.snapchat.com/en-US https://netsonly.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 WHATSAPP

UK AND EUROPE 16+ 13+ REST OF THE WORLD

WhatsApp is the world's most popular messaging service, with around two billion users exchanging texts, photos, videos and documents, as well as making voice and video calls. Its end-to-end encryption means messages can only be viewed by the sender and any recipients: not even WhatsApp can read them. Updates to its privacy policy in 2021 (involving sharing data with parent company Facebook) caused millions to leave the app, but the new policy was widely misinterpreted – it only related to WhatsApp's business features, not to personal messages.

SCAMS

Fraudsters occasionally send WhatsApp messages pretending to offer prizes – encouraging the user to click on a link to win. Other common scams involve warning someone that their WhatsApp subscription has run out (aiming to dupe them into disclosing payment details) or impersonating a friend or relative and asking for money to be transferred to help with an emergency.

DISAPPEARING MESSAGES

Users can set WhatsApp messages to disappear in 24 hours, 7 days or 90 days by default. Photos and videos can also be instructed to disappear after the recipient has viewed them. These files can't be saved or forwarded – so if your child was sent an inappropriate message, it would be difficult to prove any wrongdoing. However, the receiver can take a screenshot and save that as evidence.

ENABLING FAKE NEWS

WhatsApp has unfortunately been linked to accelerating the spread of dangerous rumours. In India in 2018, some outbreaks of mob violence appear to have been sparked by false allegations being 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.

POTENTIAL CYBERBULLYING

Group chat 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.

CONTACT FROM STRANGERS

To start a WhatsApp chat, you only need the mobile number of the person you want to message (the other person also needs to have the app). WhatsApp can access the address book on someone's device and recognise which of their contacts also use the app. So if your child has ever given their phone number to someone they don't know, that person could use it to contact them via WhatsApp.

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." It is a useful method for a young person to let loved ones know they're safe – but if they used it in a chat with people they don't know, they would be exposing their location to them, too.

Advice for Parents & Carers

CREATE A SAFE PROFILE

Even though someone would need a child's phone number to add them as a contact, it's also worth altering a young person'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 that your child's profile is better protected.

EXPLAIN ABOUT BLOCKING

If your child receives spam or offensive messages, calls or files from a contact, they should block them using 'settings' in the chat. 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 – so they also need to be deleted from the address book.

REPORT POTENTIAL SCAMS

Young people shouldn't 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'll be given the option to report it as spam. If the sender claims to be a friend or relative, call that person on their usual number to verify it really is them, or if it's someone trying to trick your child.

LEAVE A GROUP

If your child is in a group chat that is making them feel uncomfortable, or has been added to a group that they don't want to be part of, they can use WhatsApp's group 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.

THINK ABOUT LOCATION

If your child needs to use the 'live location' function to show you or one of their friends where they are, advise them to share their location only for as long as they need to. WhatsApp gives a range of 'live location' options, and your child should manually stop sharing their position as soon as it is no longer needed.

DELETE ACCIDENTAL MESSAGES

If your child posts a message they want to delete, WhatsApp allows the user seven minutes to erase a message. Tap and hold on the message, choose 'delete' and then 'delete for everyone.' However, it's important to remember that recipients may have seen (and taken a screenshot of) a message before it was deleted.

CHECK THE FACTS

You can now fact-check WhatsApp messages that have been forwarded at least five times, 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 true or not.

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

What Parents & Carers Need to Know about DISCORD

AGE RATING 13+

Servers and channels marked as 'NSFW' require users to be 18 or older to join.

Discord is a free app which allows users to communicate in real time via text, video or voice chat. Available on desktop and mobile devices, it was originally designed to help gamers cooperate – but has evolved into a more general networking platform for a range of online communities, discussing topics like TV series, music, Web3 and more. Discord is organised around closed groups, referred to as 'servers'. To join a server, users must be invited or provided with a unique link. It's a space for users to interact with friends, meet others with shared interests and collaborate privately online – but it's also a place where young people can be exposed to risks if the right precautions aren't taken.

WHAT ARE THE RISKS?

CYBERBULLYING

Discord's easy accessibility and connectivity, unfortunately, makes it an ideal place for cyberbullying to occur – especially as audio and video streams disappear once they've ended, meaning that bullying could take place without leaving any evidence. Closed groups can also be created, giving young people the opportunity to exclude their peers or send cruel messages without adult oversight.

DIFFICULT TO MODERATE

Like many private communication apps, Discord's real-time messaging can be difficult to control. The system enables content moderation through each individual server – so different groups can set their own rules for what's acceptable, and some groups may not monitor for unsuitable content. Anything that happens in an audio or video stream is also virtually untraceable once the stream has concluded.

INAPPROPRIATE CONTENT

Discord mainly hosts private groups, making it easier for unsuitable or explicit content to be shared on channels. Pornography, racism and inappropriate language can be found in some groups. Server owners are required to add an age-restriction gate to channels where 18+ content is being shared – but this solution isn't foolproof, as the platform doesn't always verify users' ages when they sign up.

ACCESSIBLE TO PREDATORS

On many chat platforms, users can lie about their age or true identity – and Discord is no exception. Predators have attempted to abuse the platform by using it to contact and communicate with underage users – by initially chatting with a child on an age-appropriate channel, for example. While Discord has improved its safety settings, some users will still try to bypass them for malicious reasons.

CRIMINAL ACTIVITY

Discord does have strict Terms of Service and Community Guidelines to protect its users – but, sadly, not everyone adheres to them. Criminal activity including grooming, hate speech, harassment, exploitative content, doxxing and extremist or violent material have all been found on Discord servers over the last two years. In 2020, Discord received almost 27,000 reports of illegal activity on the platform.

Advice for Parents & Carers

REVIEW SAFETY SETTINGS

Discord has a series of safety settings, enabling users to choose who can direct message them or send them friend requests. Your child's experience on Discord will be much safer if the app's privacy and safety settings are configured to only allow messages or friend requests from server members. This will minimise the chances of potential predators from outside the group contacting them.

EXPLAIN AGE FILTERING

While Discord requires users to be at least 13 to sign up, many servers geared towards older users are flagged as NSFW (not safe for work), which indicates they probably contain material that's inappropriate for children. It can be easy to click through settings without properly reviewing them, so ensure your child understands why age filtering is important and that it's there to protect them.

SCREEN OUT EXPLICIT CONTENT

In the privacy and safety settings, Discord users are offered the ability to filter direct messages for inappropriate content: a setting that should be enabled if your child uses the platform. Discord automatically tries to flag images that are explicit, but the setting must be manually enabled for text. If a young user is sent explicit content in a direct message, Discord will scan and (if necessary) delete it.

MONITOR ONLINE ACTIVITY

It's wise to regularly review your child's activity on Discord. This can include checking their safety settings to ensure they're correctly enabled, talking about which servers they've joined and reviewing some of their friends and direct messages. Ask if anything has made them feel uncomfortable or unsafe. Things can change quickly online, so plan routine check-ins and follow up frequently.

DISCUSS GOOD ONLINE BEHAVIOUR

The anonymity offered by the internet often leads people to communicate more openly online and behave differently than they would at school or home. It's crucial to bear in mind, though, that every internet user is still a real person. Talk to your child about the severe and lasting consequences that cyberbullying or exchanging inappropriate material online can have in the real world.

HAVE CANDID CONVERSATIONS

It can sometimes be awkward to discuss topics like grooming, pornography, racism or explicit content with your child – but it's important to ensure they're aware of the harms these things can pose. Talking openly about these subjects is a great way to help your child feel more comfortable about coming to you if they experience an unwanted encounter on Discord (or anywhere else online).

Meet Our Expert

Coral Cripps is a Canadian-born, London-based tech journalist at gmw3.com: a website specialising in all things Web3, gaming and XR (extended reality). With a focus on brands and culture, she researches and writes about the ways that our current innovations – including the metaverse and Web3 – are impacting people, places and things.

National Online Safety

#WakeUpWednesday

How you can support your child

- **Close down all social media accounts for a period of time.**
  This allows for previous content to be removed in the case of harassment or bullying.
- **Understand algorithms and the impact these can have.**
  If a student has searched something like self-harm or depression this will be picked up and their feed will then be automatically flooded with this type of content.
- **Try and encourage openness and good communication.**
  Regular chats about online activity is good practice. It allows you to remind them about only speaking with people they trust and not sharing passwords

How you can support your child

- **Put together an agreed plan for time spent online.**
  Look at screen time limits and times to disconnect.
- **Turn off push notifications.**
  Removing the reminders or prompts of updates helps to reduce the amount spent checking your phone.
- **If you have any concerns about any websites or social media platforms report them to CEOP.**
  This can be done on the website. Alternatively you can block users or report accounts. If things escalate you can report incidents to 101.

World-class learning	The highest expectations	No excuses	Growth mindset	Never give up	Everyone is valued	Integrity
World-class learning every lesson, every day	Everyone can be successful; always expect the highest standards	Create solutions not excuses; make positive thinking a habit	Believe you can improve; work hard and value feedback	Resilience is essential; be relentless in the pursuit of excellence	Diversity is celebrated; see the best in everyone	Be trustworthy and honest; deliver on promises and walk the talk

MALTBY LEARNING TRUST
Exceptional Experiences. Successful Lives.

How you can support your child

- **Be prepared to listen.**
  Actively listen and try not to show judgment or criticism.
- **Seek expert advice – National Online Safety / Internet Matters / NSPCC.**
  If you are unsure on how to deal with a situation have a look at these website for some guidance or advice.
- **Perform random checks on their phones and walk abouts when they are facetiming.**
  This will help you to feel better about keeping an eye on what they are doing…….just be prepared for the odd swear word!

World-class learning	The highest expectations	No excuses	Growth mindset	Never give up	Everyone is valued	Integrity
World-class learning every lesson, every day	Everyone can be successful; always expect the highest standards	Create solutions not excuses; make positive thinking a habit	Believe you can improve; work hard and value feedback	Resilience is essential; be relentless in the pursuit of excellence	Diversity is celebrated; see the best in everyone	Be trustworthy and honest; deliver on promises and walk the talk

MALTBYLEARNINGTRUST
Exceptional Experiences. Successful Lives.