What Parents & Carers Need to Know about

AMIGO

Amigo is a social platform which purports to connect strangers from around the world – and, with built-in translation software, it reduces the expected language barriers. Focusing heavily on one-to-one chat, video calls and live streams, Amigo encourages its users to build up online relationships and unlock exclusive features such as private video and audio calls: essentially, the more that people chat, the more functions become available to them. This is an app designed with mature users very much in mind and is therefore definitely not recommended for children.

AGE RATING 18

WHAT ARE THE RISKS?

ONE-TO-ONE COMMUNICATION

While online chats and livestreaming are a great way to communicate with people that children can trust (such as friends and family), Amigo encourages users to connect with complete strangers and develop a friendship through private chats, calls and videos. This will be a clear red flag for most parents, due to the possibility of a child encountering inappropriate content or an online predator.

INAPPROPRIATE CONTACT

Within minutes of signing up for our trial of Amigo (and without using a profile photo), users of the opposite sex were messaging with suggestive statements such as "You're just my type" and "Let's have fun". While the app's stated intent is to help people build friendships, some users obviously seek to take those relationships in a more mature and amorous direction.

MEMBERSHIP COSTS

Like many apps that are free to download, Amigo's business model is centred on in-app purchases. Users are encouraged to pay for VIP membership – enabling them to send more messages each day and boosting their profile's visibility. People can also buy coins (again, for real money) which allow them to send virtual gifts and further increase the number of messages they can send daily.

LACK OF AGE VERIFICATION

Amigo makes no secret of the fact that it's for people aged 18 or above. There's no age verification, however, so a young person could simply sign up under a false date of birth. The app's algorithm claims to match users of similar ages (making them more compatible), but either the algorithm isn't very reliable, or most users have entered a fake age which doesn't correspond with their profile pic.

REWARDS FOR REPEATED USE

Amigo gifts virtual coins to users if they reply to messages within 10 seconds, while there are also daily rewards for posting comments, sharing a video, getting likes or simply opening the app. It also encourages increasing 'Intimacy Levels' with other users to unlock extra features: once someone's online 'friendship' reaches Intimacy Level 3, they can hold one-to-one video calls with each other.

Advice for Parents & Carers

MONITOR DOWNLOADS

As well as frequent catch-ups with your child about what they've enjoyed doing online, you could consider taking the additional step of physically checking their phone every so often to see which apps they've installed. The safest option could be to enable 'ask to buy' (Apple) or 'purchase approvals' (Android) on their device, meaning your authorisation is needed to download any apps.

BLOCK, REPORT, DISCUSS

Many children already know that connecting with strangers online is dangerous, but it never hurts to refresh their memory. Whatever communication apps your child uses, make sure they're fully aware that if anything online makes them feel uncomfortable, scared or upset, then they can block the user responsible, report the content, take a screenshot as evidence and come to tell you straight away.

RESPECT AGE RESTRICTIONS

Apps have age restrictions for a reason, and Amigo is very definitely a mature content platform. Given that many of Amigo's users apparently use a bogus date of birth, you might want to remind your child about the implications of setting up a fake profile – such as being exposed to messages and videos that make them feel uncomfortable or feeling pressured into chatting with strangers.

ACTIVE LISTENING

If your child *does* approach you with a concern, make time to stop what you're doing and actively listen. Let them talk without interrupting or showing any judgement, then discuss their options and the possible solutions: this empowers them and reassures them that you're there to be supportive. If the issue is one that has put your child at risk, however, you may wish to contact the police.

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.

Sources: https://apps.apple.com/us/app/amigo-chat-rooms-real-friends/id1555401554

National Online Safety®

#WakeUpWednesday

What Parents & Carers Need to Know about

BEREAL

BeReal is the latest trending social media app. The concept is that people see others in their authentic day-to-day lives, sharing candid photos without editing or applying filters. Each day at a random time, users are simultaneously notified to take a picture of what they're doing at that exact moment. The two-minute window to submit an image means there's no time to select a particularly glamorous or exciting activity. BeReal shares two pictures: a selfie, and an image of the immediate surroundings. Users can only view and react to their friends' photos once they upload their own.

AGE RATING 13+ from the App Store & Google Play

WHAT ARE THE RISKS?

CONTINUOUS NOTIFICATIONS

Like any social media app, BeReal's developers want users to be on it regularly and scrolling for long periods. BeReal only sends one notification to post a picture each day, but there are other alerts for events such as mentions, comments, friend requests and reactions to your photo. This can cause young users to feel pressure to open the app and respond, distracting them from other activities.

EASY LOCATION

BeReal's default setting is to share the exact location of where a post was sent from. Given that images are usually shared within the two-minute window, anyone your child is friends with on the app will know exactly where they are (or at least, where they *were* two minutes earlier). As we've noted, this could include strangers who are intending to use this geographical information for malicious purposes.

CONNECTING WITH STRANGERS

When someone signs up to BeReal, it highlights anyone in their phone's contacts list who already has the app – so users can connect with friends, or invite others from their contacts. The 'Discovery' feed, meanwhile, shows posts from strangers and gives users the option to add them as friends, too. This means your child could potentially connect with – and communicate with – a stranger.

VISIBLE PERSONAL DATA

As with any other form of social media, it's important that your child doesn't share too much personal information on their profile. BeReal allows for a photo, full name, approximate location and a short bio. It's safest to make sure that your child's profile doesn't display anything which could identify where they go to school or exactly where they live.

PUBLIC SHARING

As well as sharing posts with friends in the moment, the app also allows posts to be shared publicly and public content to be viewed. Before a user can see this public content, they must post their own photo first. Unfortunately, there currently seems to be a lack of moderation on the content that's being uploaded, so a young user could be exposed to posts which aren't suitable for their age.

REPUTATIONAL DAMAGE

What your child says and does online – their digital footprint – shapes the way that other people see them. It's essential that young people understand that when they post something online, they are giving the app in question the right to do whatever they wish with that image or content, including sharing it elsewhere. This form of permission is explicitly referenced in BeReal's terms of use.

Advice for Parents & Carers

LIMIT NOTIFICATIONS

BeReal offers the option to turn off individual types of notification. Doing this will significantly reduce the number of times your child is tempted to open the app by incoming comments, uploads, friend requests and so on. Ironically, it will allow them to actually 'be real' by being present in the moment and their current environment as opposed to being engrossed on social media.

KEEP IT AMONG FRIENDS

Remind your child why adding strangers to their contacts isn't a good idea, and advise them to decline any friend requests from people they don't know in real life. If something your child sees on BeReal makes them feel uncomfortable, they can report it by clicking on the three dots in the top right. The reporting tool allows them to state the reason that they're flagging up the post.

STOP AND THINK

BeReal's goal is for users to be authentic with friends, removing the pressure of that flawless photo or perfectly worded post. It's still vital, though, that children stop and think rather than uploading something risky just to meet the two-minute deadline. Point out to them what kind of information strangers could extract from an image: school crests, street names or local landmarks, for example.

CREATE A SAFE PROFILE

Remind your child to use an avatar as their profile pic (as opposed to a photo of themselves) and use a nickname or just their first name, not their full name. Any information they add to their bio (which is optional) should be kept vague, and personal details should remain private. It's also worth turning off the geolocation feature either through the device's settings or in BeReal itself.

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.

Sources: https://bere.al/en/privacy | https://bere.al/en/terms
https://berealapp.notion.site/FAQ-BeReal-English-2d1d59a4168c4524bed0a40b04de892a | https://www.commonsensemedia.org/app-reviews/bereal

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

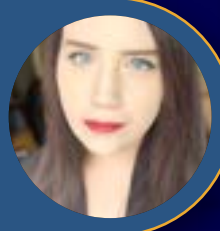
The anonymity offered by the internet often leads people to communicate more openly online and behave differently than they would at school or home. It's crucial to bear in mind, though, that every internet user is still a real person. Talk to your child about the severe and lasting consequences that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



Sources: https://www.defendyoungminds.com/post/dangers-of-discord-6-steps-safeguarding-teens-on-popular-chat-app | https://support.discord.com
https://endsexualexploitation.org/articles/discord-is-a-haven-for-gamers-and-sexual-exploiters/ | https://kotaku.com/discord-deleted-thousands-of-violent-extremist-and-crim-1846623284

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about

ECHO CHAMBERS

Digital echo chambers have become increasingly prevalent over the last half decade. Formed by a combination of social media algorithms designed to promote engagement and the basic human urge to be correct, these online environments reinforce the opinions that people already have – such as particular political ideologies – in a perpetual loop. The danger is that exposure to this constant bias can gradually nudge users towards more extreme views. That's certainly a potential hazard for young people, who tend to be more impressionable and easily influenced by things they see and read online – especially if it reflects a view they already agree with.

WHAT ARE THE RISKS?

EXTREME IDEOLOGIES

Echo chambers can offer routes to harmfully extreme worldviews. A typically teenage distrust of authority, for example, could spiral into a full-blown belief in conspiracy theories – sometimes rooted in ideas which are antisemitic, racist or misogynistic. For impressionable individuals who may be feeling disillusioned with life, echo chambers can often function as a gateway to radicalisation.

NO CRITICAL THINKING

While critical thinking skills are sometimes taught in schools, they are rarely domain specific. A lack of experience in thinking critically – for example, about things we see when browsing the internet – places young people at risk of falling prey to misinformation, untruths and false narratives, which are sometimes deliberately designed to mislead them and influence their thinking.

A VALUES VACUUM

If schools struggle to deliver on a clear ethos, founded in British values as outlined in the national curriculum, it leaves a space within which other ideologies have potential to flourish. Teaching about British values in more siloed experiences, such as PSHE lessons, doesn't always effectively convey the key notions: tolerance, democratic values, individual liberty and the rule of law.

UNDETECTABLE INDOCTRINATION

Many people enter online echo chambers every day without realising. It's easy to simply consume whatever's placed in front of us as we keep scrolling, unaware that we're being funnelled down a particular route. Not recognising that their daily digital diet could in fact be deeply biased in favour of one side or the other can accelerate a young person's journey towards more extreme ideologies.

LACK OF BALANCE

It's challenging to reflect on your own beliefs and opinions, and question whether you might have got things wrong. That's why most of us naturally lean towards consuming information which reinforces and underlines what we thought to begin with. The long-term consequence of this is general close-mindedness and, potentially, intolerance of a more diverse set of perspectives.

Advice for Parents & Carers

TALK ABOUT CHALLENGES

It could be helpful to explain to your child that, in general, people like to find evidence to strengthen their existing beliefs and prefer to ignore anything which supports an opposing perspective. Emphasise that it's OK if someone (politely) challenges what they think occasionally, and that any criticism of their view is purely that – a criticism of their opinion, not of them as a person.

DEBATE CAN BE GREAT

Encourage any interest your child shows in debating – whether at home, at school, or in clubs or societies. Debates require people to assess the merits of an opposing argument, so they can counter it. Putting themselves in the shoes of someone who has a different point of view is a useful way for children to approach new ideas that may contradict what they previously believed.

DISCUSS 'UNHEALTHY FEEDS'

Help your child understand how online algorithms shape which information is presented to them each day: ask them to consider *why* things appear in their feed on platforms like TikTok, Instagram or Snapchat. Explain that it benefits social media companies' advertising revenue to keep people coming back by showing them content which, generally, reinforces their existing world view.

THE VALUE OF VALUES

It can be hugely beneficial if your child recognises the importance of a core set of principles, such as the British values. By regularly tying their online experiences back to those essential ideas of democracy, tolerance and kindness towards others, understanding the rule of law and protecting individual liberties, you'll be helping them grow into a more resilient and robust future citizen.

VARY THEIR DIGITAL DIET

Sitting down to read online news stories with your child is an excellent way to demonstrate to them why it's important not to always get their information from just one place. Comparing how the same story is reported across popular mainstream publications – and talking about the political biases each may have – will highlight the importance of regularly checking a wide range of online sources.

Meet Our Expert

A former director of digital learning and currently a deputy headmaster and DSL, Brendan O'Keeffe's experience and expertise gives him a clear insight into how modern digital systems impact the experience of children, staff and parents – and which strategies help to ensure that the online world remains a useful educational tool rather than a minefield of risks.

Source: https://archive.org/details/cognitiveillusio0000unse/page/79/mode/2up | https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1218526
https://www.allsides.com/media-bias/media-bias-chart

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about HiPAL

AGE RESTRICTION 12+ (with reduced functionality for under-12s)

HiPal is a trending social media app which turns phones into walkie-talkies, allowing people to have voice conversations with friends or strangers. There are two account options: one for users aged under 12 and one for those aged 12 or above. The former has fewer features and limits interaction with strangers, enabling use of the walkie-talkie feature or photo sharing with friends and family only. The 12+ accounts offer more options, including adding strangers as friends, sharing photos and videos publicly, sending private messages and holding voice chats with strangers as well as friends.

WHAT ARE THE RISKS?

CONNECTING WITH STRANGERS

HiPal's under-12 accounts don't allow direct connections with strangers (although children seeking more friends can share their 'Friend Code' on other platforms), but for older users, chatting with strangers seems to be the app's main appeal. The 'Public Square' shows nine online users (hitting 'refresh' replaces these with another nine), and clicking on someone's profile starts a conversation.

SEXTING AND SUGGESTIVE PICS

Almost immediately after our expert downloaded the app, strangers began to message privately – asking for provocative images or sharing explicit photos of themselves. Likewise, in the 'Explore' feed, many of the pictures and videos are innocent ... but some are far more salacious. There is always the risk of other users secretly saving a revealing photo and re-sharing it elsewhere.

NEED FOR VALIDATION

Some users – particularly girls – post photos on apps of this type hoping for positive reactions and comments to boost their self-esteem. Suggestive images tend to attract more flattering feedback, encouraging the user to post more frequently and with more explicit content. Conversely, receiving unkind comments about their picture can impact a young user's confidence and sense of self-worth.

NO AGE GATES OR MODERATION

Although users are given an initial choice of the under- or over-12 profile, there is no verification method to confirm someone's age; it is quite clear that the 'older' option offers a more complete experience on the app, but there seems to be no content moderation in place. Likewise, there is a reporting button for users to make a complaint but these reports do not appear to be followed up.

INTRUSIVE FEATURES

HiPal's walkie-talkie gimmick is no different from a normal phone call and seems rarely used; although it allows conversations to still be heard while a phone is locked, which could have awkward results. HiPal also offers 'Boom' messages: unmissable large-text notifications which are highly distracting and briefly take over the phone – users can't access other apps until the message fades.

LARGE GROUP CHATS

The app offers group chats with up to 100 people – both friends and unknown users. This not only means excessive 'Boom' messages taking over your child's device, but near-constant notification alerts and – most worryingly – the potential for walkie-talkie chatting and sharing photos with strangers outside parental supervision and apparently with no moderation from the platform itself.

Advice for Parents & Carers

EMPHASISE CAUTION

Remind your child of the dangers of connecting with strangers online. Some may be using the app innocently; others may have more sinister intentions. Encourage your child to consider what information they disclose in private messages and emphasise that they should inform a trusted adult if someone on the internet ever attempts to persuade them to meet in person.

TALK ABOUT SEXTING

It can be an awkward conversation (which young people are often reluctant to have), but it's vital to talk openly and non-judgementally about sexting. Discuss the legal implications of sharing explicit images, as well as the emotional impact. Make it clear your child should never feel pressured into sexting – and that they should tell a trusted adult if they receive any unwanted explicit images.

BUILD RESILIENCE

With HiPal's lack of moderation, it's imperative that children are prepared for comments they might receive after uploading an image. You can build their resilience and equip them to manage these situations by having them show you any comments they've received. Together, discuss how the nice ones made them feel – and what they could do if someone posted a comment that upset them.

AVOID OVER-SHARING

Young people should think carefully about what they share in their profile, bio and posts. Talk to your child about not disclosing personal details such as phone numbers, other social media accounts or images which could reveal where they live or go to school. It's essential for children to recognise that strangers can assemble a detailed profile of someone based on things they can find online.

CONSIDER MENTAL WELLBEING

Many users on HiPal publicly share photos that are intended to be alluring in the hope of gaining more likes, friends and positive feedback – boosting their self-esteem and making them feel more self-assured. When young people regularly engage with social media platforms, it's important that parents and carers keep in mind the potential impact such platforms can have on mental wellbeing.

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.

https://hipal.app/about/privacy.html

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about INSTAGRAM

WHAT ARE THE RISKS?

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.

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.

National Online Safety®

#WakeUpWednesday

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

What Parents & Carers Need to Know about NGL

AGE RESTRICTION 13+

NGL (which stands for 'Not Gonna Lie') is an app through which users share a link to their Instagram story or Twitter account, inviting their followers to give anonymous feedback. The app includes some prewritten questions (such as 'if you could change anything about me, what would it be?'), plus the option to ask followers to simply 'send me anonymous messages'. All replies go into the user's NGL inbox, with the sender remaining anonymous – although subscribers to the app can receive hints about who each message was from.

WHAT ARE THE RISKS?

ANONYMITY AND OVERSHARING

Anonymous messaging gives rise to the 'online disinhibition effect', which causes users to feel detached from their words and actions in the digital world. This can make young people in particular (as they tend to act more impulsively online) far more likely to disclose personal information on the internet, as well as making ill-advised confessions or revealing their fears and insecurities.

PROTECTION FOR BULLIES

Having their identity hidden makes bullies feel safe from repercussions, so anonymous chat sites are a major avenue for cyberbullying. NGL claims to use AI to filter out insulting terms, but our expert sent a range of such phrases (starting with 'cow' and 'ugly', and becoming progressively more offensive) to a 'dummy' account. All of these trial messages were delivered to the recipient's inbox.

COSTLY SUBSCRIPTIONS

NGL offers a subscription where – for a weekly fee – users can unlock hints about who's been messaging them, including the sender's approximate location and which device they used. Young people will naturally be extremely curious about who sent which message (especially if they have a lot of Instagram or Twitter followers) and may be unable to resist spending money to find out.

INFLATED ENGAGEMENT

1K

In June 2022, NGL had to revise its terms of service: informing users if a message was sent by the app's developers as opposed to genuine followers. It emerged that, previously, NGL's makers had attempted to boost engagement with the app (as well as enticing users to pay for subscriptions) by sending fake anonymous messages from bots. This update was rolled out very quietly by the team.

QUESTIONABLE SUPPORT

NGL *does* have a 'report this message' button for users to flag upsetting content. After sending a message, however, an automated reply arrives stating "... NGL is 100% anonymous and we have no way of knowing the identity of the user and would not be able to find out, even if we tried." This did not fill our expert with confidence that the app can address bad behaviour adequately.

ACCIDENTALLY GOING VIRAL

The messages on NGL itself are anonymous, but users can share these messages via their Instagram story or Twitter feed – enabling all their followers (or anyone, if their accounts are set to 'public') to see them. If a young person has disclosed something embarrassing or identifiable on NGL without realising, this information has the potential to be re-shared very quickly to a far wider audience.

Advice for Parents & Carers

DEALING WITH NEGATIVITY

Blocking another user on NGL will prevent them sending anonymous messages to your child in the short term – although a determined abuser could get around that obstacle simply by setting up a new Instagram account. If your child continually receives negative messages that upset them, it might be worth encouraging them to consider whether they really need to use the app at all.

BLOCK IN-APP PURCHASES

To avoid your child running up an eye-watering bill through an NGL subscription (or indeed any kind of costly in-app purchases), go into the settings on whatever devices they use to go online and either disable the ability to make purchases or protect that function with a password. If those options aren't available, it's prudent to ensure there aren't any payment methods linked to their account.

EXPLAIN ANONYMOUS APPS

We understand that a conversation with your child about the risks of anonymous messaging may seem difficult to initiate (especially if you aren't that comfortable with using social media yourself). It is vital, however, that young people understand that, for some people, having their identity obscured online can make them feel more powerful and less accountable for their actions.

THINK BEFORE SENDING

Regardless of whether a messaging app is anonymous or not, it's a good idea to regularly talk to your child about how it's wise to think through what they're sharing before they post it. Emphasise that nothing is truly private once it's online. If the post is something your child might hesitate to say to someone face to face, then it's probably not the sort of thing they should be writing online either.

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.

Source: https://ngl.link/#what-s_ngl

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about

SENDIT

Sendit is an add-on to Snapchat, not a standalone app: it requires users to have an active Snapchat account, which they then connect to Sendit. It's important that trusted adults realise, therefore, that any risks associated with Snapchat also affect children using Sendit. Within the app, people play question games like 'Truth or Dare' and 'Never Have I Ever': users select a question to share on their Snapchat story for their friends to reply to. All responses are anonymous, although – for paying subscribers – Sendit reveals hints about who sent which messages.

Age rating:

12+ App Store

Teen Google Play

However, Sendit's own terms and conditions state that it was developed for the 17+ age group

WHAT ARE THE RISKS?

ANONYMOUS RESPONSES

Anonymity online encourages people to say things and act in ways that they normally wouldn't. They're less accountable, and it's harder to track who sent a message. Research has highlighted that children perceive anonymous messages as being more severe than if the *same* message had come from a friend. Any app that lets children communicate anonymously should be treated with caution.

MENTAL HEALTH IMPACT

Categories of questions such as "Ask me anything" or "Rate me" – coupled with the app's anonymity – mean there is a likelihood of some friends or strangers (if the account is set to 'public') responding in a negative manner. These critical comments (especially if there are several) could ruin a young person's self-esteem – heightening their insecurities and affecting their mental health.

MEMBERSHIP COSTS

Currently costing £8.49 per week, Sendit's Diamond Membership offers clues about who sent a particular message, such as their approximate location, the type of phone used and any mutual friends. Membership also provides exclusive games and an ad-free experience. Young people may well be curious to find out who certain messages are from and therefore sign up for membership.

BULLYING AND HARASSMENT

Open-ended questions which relate personally to the sender are an opportunity for malicious people to make offensive remarks, which can lead to full-blown bullying and harassment. Additionally, bullies and trolls can hide behind the anonymity that Sendit offers, feeling more powerful and able to intimidate their target – who, by contrast, feels hurt, victimised and helpless.

POSSIBLE GROOMING

If your child doesn't have their Snapchat account set to private, or they have previously added strangers as friends, there is a possibility of predators responding to their Sendit questions. They do this in an attempt to gather information about your child – or to initiate a conversation with them, seeking ultimately to form an online 'friendship' and gain the young person's trust.

REPEATED ENGAGEMENT

On Sendit, users receive trophies for reaching a particular number of responses, for answering friends' questions and for posting their own. This sense of achievement could incentivise a young person to be active on Sendit more frequently – spending more time on their phone or tablet as they may naturally want to collect all of the trophies or might be competing with their peers.

Advice for Parents & Carers

ENCOURAGE EMPATHY

If your child has already downloaded Sendit, it might be wise to have a discussion with them about the impact that saying something anonymously online could have on others. Encourage them to think about how *they* would feel if they were on the receiving end of a particular comment. Reminding them to stop and re-read messages before sending could reduce the number of regrettable situations.

TALK IT OVER

Before allowing a young person onto a social networking app, it's a good idea to chat with them about the possibility of receiving hurtful comments. Explain that not everyone online is nice; that people often say things they don't mean; and that posts get misinterpreted. Teach your child not to reply to any offensive users on Sendit and simply block instead them (via the three dots in the top right of the screen).

BLOCK IN-APP PURCHASES

Even if you *do* allow your child to use Sendit, you might want to consider talking to them in advance about whether they really need a membership subscription. Either way, it's probably safest to make sure that in-app purchases are blocked in the settings, or that you have configured your child's device to ask for your approval before making a purchase online.

ONLY PLAY WITH FRIENDS

Stress the importance of your child playing Sendit games only with their close friends and not having strangers on their contacts list. This should help to keep the nature of the questions light-hearted – and if the games are being played among a small group, it will be easier for the members to figure out who gave certain answers if someone's been left feeling hurt or uncomfortable by any responses.

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.

Sources: https://www.getSendit.com/privacy | https://www.getSendit.com/parents | https://www.getSendit.com/terms
https://screenrant.com/is-Sendit-anonymous-on-snapchat/

National Online Safety®

#WakeUpWednesday

What Parents & Carers Need to Know about

SOCIAL MEDIA & MENTAL HEALTH

An estimated one-third of children have a social media account, so it's important that trusted adults know what content young people are consuming, what they're posting and the interactions they're having. On social media, it can be easy to go down 'rabbit holes' that aren't beneficial to our wellbeing. As platforms grapple with managing such 'legal but harmful' content, lives are being impacted – sometimes to tragic effect. We might be daunted by the scale of the tech giants and their content which so enthrals young people, but we can still help children to be aware of their mental wellness: recognising when something isn't OK ... and knowing what to do about content that upsets them.

1. UNDERSTAND THE ALGORITHM

Algorithms rank content by user interest: someone who regularly interacts with sports news, say, will see the latest results at the top of their feed. Likewise, if a user browses content that can cause harm, that's what will be recommended to them in future. Someone who's had a bad day and looks for posts which reflect their mood will find similar content being suggested to them more and more.

2. AVOID THE MAIN FEEDS

Avoiding the default feeds on social media platforms limits the amount of recommended content that's shown. Users can opt to only scroll through the accounts they follow, use restricted modes, or highlight posts that they don't want to see more of. Explore the platform safety settings to see how you can take control of what your child's phone shows them when they open the app.

3. DISCUSS WHAT THEY'VE SEEN

Chatting about what your child's seen online keeps you aware of the content they're interacting with. Don't assume that platforms are screening out inappropriate material, or even that your child would recognise content as being harmful. Discuss who they follow, what posts they like and what comes up in their feeds: if alarm bells ring, it could be time for a more in-depth talk or to seek support.

4. LEARN HOW TO HIDE CONTENT

If your child stumbles across unsuitable content on social media, there's the option to hide that post as well as indicating you'd prefer any similar material not to be suggested in future. On some platforms, you might also be able to block posts that contain specific words, which is an excellent way to start taking control of what your child sees online.

5. SET DAILY LIMITS

Phones and most apps can tell you how much they're being used. Spending too long online can mean a child misses out on other activities that are important to all-round wellbeing. You could set some family rules – for everyone to follow – around device use, such as screen time limits and tech-free spaces: involving your child in creating this agreement makes them more likely to stick to it.

6. MONITOR THEIR ACTIVITY

Keeping a discreet eye on how your child is using social media can help ensure they're not entering potentially dangerous situations. As they grow up, of course, children need space to exercise their independence – but you can still occasionally ask to see what they're looking at. Be transparent about your own social media use and try not to sound judgemental about your child's.

7. TURN OFF PUSH NOTIFICATIONS

Even for adults, it's tempting to check an email or message as soon as the alert sound pings. Push notifications encourage people to open their apps and spend time on their device, so turning them off will help your child to practise mindful use of tech. Most of us have other things that we need to focus on as a priority – and those notifications will still be there later, when we have more time.

8. USE DEVICES TOGETHER

Giving children internet-enabled devices and complete freedom to explore platforms on their own can result in exposure to hugely damaging content. You could consider making a particular area at home a designated space to use phones, tablets and so on – making it much easier to monitor what content your child is viewing and (if necessary) steer them away from any potentially harmful paths.

9. ENCOURAGE OTHER ACTIVITIES

Mental health professionals often highlight the importance of exercise, quality time with loved ones, a balanced diet and restful sleep for our mental wellbeing. Spending hours on social media can cause us to sacrifice other activities that our brains need to feel well – so encouraging your child to put down their phone and enjoy something that doesn't involve a screen can be immensely beneficial.

10. TALK ABOUT PEER PRESSURE

Most platforms default children's accounts to private, so only people they've accepted as friends can see their posts. This reduces the risk of bullying or unkind comments, but – just like offline life – the digital world can still make children feel as if they need to act or look a certain way to fit in. Talk to your child about peer pressure, and listen to any concerns so you can provide the support they need.

Meet Our Expert

Shazia Sarwar-Azim is executive headteacher at a specialist primary school and, as an emotional therapy coach, works with school leaders to focus on the SEND, mental health and wellbeing agenda. A passionate advocate for vulnerable learners, Shazia is a Fellow of the Chartered College of Teaching and the author of The Rainbow Within, a book which supports children with SEMH needs.

Sources: https://www.bbc.co.uk/news/technology-63204605
https://sproutsocial.com/insights/social-media-algorithms/

National Online Safety®
#WakeUpWednesday

What parents & carers need to know about...

TELLONYM

17+

Tellonym is a messaging network that allows children to send messages to each other anonymously. Users are encouraged to share their Tellonym link with others through social platforms like Snapchat, Twitter, and Instagram, and wait for friends to reply to questions anonymously. The app is free to download from both the Google Play and Apple Store and is very similar to the Sarahah app that was removed in 2018 due to repeated incidents of online bullying and inappropriate use.

Online bullying concerns

Like many other anonymous messaging platforms that exist, Tellonym can encourage online bullying behaviour. The security of remaining anonymous means that some users may use the platform to send hurtful messages or insults to others, knowing that they are unlikely to be caught or face any serious consequences. In 2018, the app received national attention for its potential to facilitate cyberbullying.

Inappropriate content

Anonymous messaging platforms such as Tellonym can also open users up to receiving age-inappropriate or sexually motivated content. Whist the app does offer moderation tools and the ability to filter explicit language, it can be linked to social media accounts such as Twitter, Instagram, and Snapchat, which means inappropriate messages can also be accompanied by inappropriate visual content.

Risk of online grooming

Users can create a Tellonym account using their email address or mobile number. All profiles created on Tellonym are automatically made public on the account and cannot be privatised. This means that children can easily be found by other users and can receive anonymous messages directly from others, leaving them susceptible to being exploited by online groomers.

Can impact mental health

Anonymous apps have in the past been linked to causing teenage depression and suicide, as children ask more personal questions and find it hard to manage negative responses. Both Ask.fm and Sarahah received widespread publicity in the past for their role in facilitating harmful behaviour, with the latter eventually banned from the Apple and Google store after a successful petition to have it removed.

National Online Safety®
#WakeUpWednesday

Safety Tips

Talk about the risks

It's important to educate your child about the risks associated with anonymous messaging apps and how other users might use it as a vehicle to send abusive or inappropriate messages. If your child is insistent on using Tellonym, explore it with them and discuss how it works and how they should use it. Always make sure they feel comfortable speaking to you about any concerns they have and that they can come to you if something upsets or worries them.

Set language filters to very high

Tellonym allows users to set different language filter levels to help protection children against receiving any spam, offensive messages or being sexually harassed. If your child is using Tellonym, it's a good idea to set these to very high, at which point content will be filtered on 'what may not be appropriate' rather than 'what is presumably not appropriate' if just set to high.

Use Custom Word Filter

Parents can add words to their children's custom word filter to exclude specific topics completely. If messages include that exact word, it gets instantly removed without further notice. This way you can control which messages your child receives. General harsh language is already filtered, so Tellonyn recommends to add words that are connected to inappropriate messages that your child might receive.

Report tells and block users

If your child receives any inappropriate messages, they can be reported directly to Tellonym on the app. Similarly, Tellonym has blocking mechanisms to exclude people you don't want your child to interact with. This removes their ability to see your child's posts and interact with them. Furthermore, you can block senders of individuals tells which will remove their ability to comment on anything further.

Stick to the age rating

Tellonym requires users to be 17 years of age or older. This reflects the nature of content that is available on the app and what younger children might be exposed to. Children who are under the age limit require an adult to email Tellonym directly confirming they have been provided with permission to use the app.

Keep personal profile private

When signing up with Tellonym, the profile page allows users to display a picture and enter their name, gender, phone number and email address. It also asks users to create a username. Given that all profiles on Tellonym are public, it's important to talk to your child about protecting their personal information and restricting the details they provide. The use of avatars and using randomly generated usernames are a good way to keep identities hidden.

Meet our expert

Jonathan Taylor is an online safety, social media and online grooming expert who previously worked as a Covert Internet Investigator with the Metropolitan Police for over 10 years. He has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, apps and platforms.

What Parents & Carers Need to Know about TIKTOK

AGE RESTRICTION 13+ (certain features are restricted to over-18s only)

TikTok is a free social media platform that lets users create, share and watch short videos ranging anywhere from 15 seconds to 10 minutes in duration. The app gained notoriety for its viral dances, trends and celebrity cameos and can be a creative, fun platform for teens to enjoy. Now available in 75 languages, it has more than a billion active users worldwide (as of spring 2022) and is most popular with the under-16 age bracket. In fact, a 2022 Ofcom report found TikTok to be the most-used social media platform for posting content, particularly among young people aged 12 to 17.

WHAT ARE THE RISKS?

AGE-INAPPROPRIATE CONTENT

While TikTok's "Following" feed only displays videos from users someone follows, "For You" is a stream of clips based on their previously watched content. Most videos on a child's "For You" feed will therefore be light-hearted and amusing, but it *could* potentially surface something unsuitable. TikTok's guidelines prohibit the sharing of illegal or inappropriate content, but the sheer volume of uploads mean they aren't manually monitored and vetted.

18 CENSORED

DANGEROUS CHALLENGES

Due to TikTok's immense popularity, some young people have unfortunately been influenced by videos challenging them to perform harmful, criminal or even deadly acts. One extreme example was the 'blackout' trend, which encouraged users to hold their breath until they passed out from a lack of oxygen. It led to two families filing lawsuits against TikTok over the tragic deaths of their children.

CONTACT WITH STRANGERS

With around 1.1 billion users globally, the potential for contact from strangers on TikTok is high – especially as accounts created by over-16s (or youngsters using a false date of birth) are set to public by default. This not only means that someone's profile is visible to everyone else on the app: it also lets their videos be suggested to others and enables anyone to comment on them or download them.

IN-APP SPENDING

TikTok is free, but users have the option to buy TikTok coins, which can be used to purchase emojis in the app. These emojis are then sent as rewards (retaining their monetary value) to other users for videos they've created. Coin bundles range from £9.99 to an eye-watering £99; TikTok's policy is that they can't be bought by under-18s, but it's possible to bypass this with a fake birthdate.

ADDICTIVE NATURE

Like all social networking platforms, TikTok can be addictive: figures show that young people are investing increasing amounts of time in it. In the UK, children with TikTok spend an average of 102 minutes per day on the app, versus 53 minutes on YouTube. This compulsive repeated use can interfere with their sleep patterns – leading to irritability – and distract them from other activities.

TIKTOK NOW

Introduced in late 2022, the 'TikTok Now' feature lets users post a daily video or photo at the exact same time as their friends. Users receive a synchronised notification at a random time of day, giving them three minutes to take a video or real-time photo. This addition can not only be a distraction to young people but could lead to them inadvertently sharing private content such as their location.

Advice for Parents & Carers

ENABLE FAMILY PAIRING

Family Pairing allows parents to link their TikTok account with their child's and control their settings remotely. Parents can then, for example, turn on Restricted Mode (reducing the chances of a child seeing inappropriate content); set screen time limits; and manage their child's ability to send messages (and to whom). Children can't alter these settings without parental approval.

MAKE ACCOUNTS PRIVATE

Although under-16s will have their TikTok account set to private by default, bypassing this setting is relatively easy. However, parents have the ability to manually set their child's account to private – meaning that their videos won't be visible to strangers and they won't be able to exchange messages with people who aren't on their friends list.

LIMIT IN-APP SPENDING

If your child is using an iPhone or Android device to access TikTok, you can alter the settings to prevent them from making in-app purchases. We'd recommend that you enable this feature, as it's quite easy for a young person – without realising what they're doing – to spend a significant amount of real money buying TikTok coins so they can unlock more features of the app.

DISCUSS THE DANGERS

If your child wants to use TikTok and you're happy for them to do so, it's crucial to talk about the potential risks in this type of app. For example, ensure they understand not to share any identifying personal information – and that they realise they could be exposed to inappropriate content. Thinking critically about what they see on TikTok can help children become generally more social media savvy.

READ THE SIGNS

If you're concerned that your child might be spending too much time on TikTok, or that they've been emotionally affected by something inappropriate or upsetting that they've seen, it's important to know how to spot the possible signs. Increased irritability and a lack of concentration are potential red flags, as are failing to complete homework or regularly not eating meals.

Meet Our Expert

Carly Page is an experienced technology journalist with a track record of more than 10 years in the industry. Previously the editor of tech tabloid The Inquirer, Carly is now a freelance technology journalist, editor and consultant.

NOS National Online Safety

#WakeUpWednesday

What Parents Need to Know about TINDER

WHAT IS TINDER?

Tinder is a free online mobile dating app regularly used by more than 60 million people worldwide. Users sign up and are matched with other people based on various preferences, such as location, age and shared interests. The user can swipe right to show interest in a profile (and connect as a match) or swipe left to ignore (decline) the match. If two users both like each other's profile and become a match, they are then able to communicate with each other directly. Tinder is officially for over 18s only – but until very recently, the age verification was easy to bypass and therefore Tinder is likely to have a proportion of users who are under 18.

AGE RATING 18+

USING THE APP ...

FAKE PROFILES

Tinder doesn't require much information for a user to create a profile, which means that there's no verification of people's details. Therefore, you may have very limited information about who you are actually speaking to. This can include not knowing the real age or identity of a person that you're matched with – making it far easier to be taken in by fake profiles.

PRESSURE TO MEET

While people *can* find love through the app, Tinder has become synonymous with casual or short-term relationships. It allows for quick conversations which can put pressure on matches to meet up as soon as possible. This may put young users at risk of meeting individuals they don't know much about or who are only looking for sexual encounters.

PRIVACY CONCERNS

Tinder let users share some of their personal details – such as name and age – and link their Tinder account to Facebook. The app allows searches of a specific location, which could lead to a user discovering a young person's exact location. It's also possible that photos uploaded to Tinder could be saved and used in other ways without consent or notification.

UNDERAGE USE

Before raising the age limit to 18 in 2016, Tinder itself admitted a proportion of its users were in the 13–17 bracket. Evidence suggests the app remains popular with teens: Tinder has recently improved its age verification, but many under 18s had already joined using a false date of birth.

EMOTIONAL HARM

The idea of instant feedback and satisfaction can put young people at increased risk of emotional harm. They may feel pressure to look or act a certain way and with begin to measure their self-worth based on how many matches they receive. This can have a negative long-term influence on young people's mood, self-esteem and confidence. It also strongly implies that compliance is a way to fit in and be liked.

Advice for Parents & Carers

COMMUNICATE OPENLY

Be candid with teens about the possibilities of online dating – but also discuss the potential dangers. An honest chat can help them feel more comfortable about coming to you with any future worries or concerns. This can reduce any stress they are feeling and increase their sense of security.

REPORT AND BLOCK

Tinder gives users the option to "unmatch" with someone they have previously connected with, as well as to report any inappropriate interactions they experience. If an account appears to be suspicious, then it's important teens are aware that they can unmatch with a user, block them and report them to the app itself. They can also report any inappropriate or offensive messages.

AVOID OVER-SHARING

Teenagers should seriously consider what they include on a Tinder profile. They should never disclose sensitive details – and be cautious about sharing their phone number, date of birth, email address and location. Using different profile pictures on their various social media accounts makes it tougher for someone to track them down.

MONITOR EMOTIONAL HEALTH

With cyber bullying presenting a significant risk, it's important that young people stay aware of their own emotional state. How do they feel before and after they use Tinder? Help them to identify when it might be time to take a break from the app and consider ways they can improve their mood. They should also know who they can speak about how they are feeling or any negative experiences they may have online.

BUILD IN SAFEGUARDS

It's vitally important that young people take precautions if they want to meet up with someone from Tinder. This should include meeting in an extremely public place and telling a friend or family member where they are going in advance. It may be useful to decide on a code word that a young person can include in a text or call to their friend or family member, to signal that they feel unsafe on the date.

Meet Our Expert

Dr Rina Bajaj is a Counselling Psychologist who has worked in mental health since 2004 (for the NHS, statutory organisations, in the corporate world and the voluntary sector). Her areas of specialism include dating and relationships counselling, and she has diverse experience in helping people from a range of backgrounds.

SOURCES: https://tinder.com | https://apps.apple.com/us/app/tinder-dating-new-friends/id547702041
https://www.theguardian.com/technology/2014/feb/24/tinder-dating-app-social-networks

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about

TWITTER

AGE RESTRICTION 13+

Twitter is a social media network which allows users to post short messages ('tweets') of up to 280 characters. Tweets can consist of text, photos, videos, audio, links, polls and GIFs – often linked by hashtags if they share a common theme or message. Hashtags receiving high levels of interest are said to be 'trending'. Twitter users can engage with other people's posts by liking, retweeting (sharing) or tweeting back (commenting on). Since the entrepreneur Elon Musk acquired Twitter in October 2022 for $44 billion, he has implemented several major changes to the platform.

WHAT ARE THE RISKS?

INTERACTION WITH STRANGERS

Tweets are public by default, meaning that anyone can view and interact with posts, follow someone and send direct messages. The concern here is that young people may therefore connect and communicate with strangers. Some individuals may follow a young person's Twitter account simply because they have similar interests; however, others may turn out to have more sinister intentions.

FIXATION ON VIEW COUNT

Twitter has recently introduced a 'view count' feature – telling users how many people have seen their tweet (even if they haven't reacted to it). Previous research has found that unfavourable comparisons with other social media users can cause young people to experience feelings of insecurity, jealousy and low self-esteem – leading to an obsession with increasing their numbers.

TROLLS AND BULLYING

The anonymity offered by fake profiles encourages some users to send tweets designed to provoke a reaction; to disrupt conversations; to spark an argument; or to harass the recipient. Such trolling and bullying can impact the mental wellbeing of both the target and anyone who witnesses it. Encourage your child to come to you if they experience such behaviour on Twitter, or if they see it taking place.

PAID-FOR VERIFICATION

Previously, if a Twitter profile displayed a blue tick icon, it meant that the owner – usually a celebrity or a major organisation – had been verified as genuine. Now, however, anyone can pay for a Twitter Blue subscription to receive the tick, with the platform carrying out limited checks on the account's authenticity. This could easily lead to more fake accounts impersonating real people or companies.

CONTENT MODERATION CHANGES

In late 2022, Twitter stated that their "policy enforcement will rely more heavily on de-amplification of violative content: freedom of speech, but not freedom of reach". No policies have changed yet, but this wording suggests they may limit who can see posts rather than removing them. While supporting free speech, this could encourage an environment where some toxic content remains online.

HIJACKED HASHTAGS

The hashtag (#) is one of Twitter's most recognisable facets, allowing users to find specific trends or topics. But the sheer volume of tweets each hour can rapidly distort a hashtag's meaning: an initially innocent search term can quickly end up returning inappropriate results. This is common with 'trending' hashtags, as people know that using them will get their tweet seen by a larger audience.

Advice for Parents & Carers

SET ACCOUNTS TO PRIVATE

To reduce some of the fear of your child's tweets being seen and shared by anyone, you can always make their account protected. This means that your child has to give approval for another user to view their posts. You can change Twitter's privacy settings so that your child can't be messaged directly by other people on the platform and their geographical location won't be shared.

FOSTER CRITICAL THINKING

It can be difficult for *anyone* to ascertain if something online is real or false, but particularly for young people. Encourage your child to check several reputable sources to determine if a story they've seen is true; remind them to watch out for scams and think about the message's possible motive. Emphasise that it's not a good idea to retweet something if they aren't sure it's correct.

ENGAGE SAFETY MODE

When Safety Mode is activated, Twitter checks for abusive or spammy behaviour such as hurtful language or repeated negative replies. The platform then flags these suspect accounts and blocks them from responding to your child's tweets. The autoblock function then prevents these accounts from interacting with your child's again for seven days.

EXPLORE THE NEW SETTINGS

Previously, any user could reply to anyone else's tweets. However, the new conversation settings let your child determine who can reply to their posts – either by selecting everyone (the default option), people they follow or only people they mention (using the @ symbol). This improvement has given users extra control, providing them with more protection from trolls and online abuse.

PAUSE BEFORE POSTING

It's important that young people think about what they're about to post and whether they might regret it later. Twitter has developed 'nudges': little prompts which appear if someone is about to tweet using harmful or offensive language. These nudges promote more positive online behaviour by giving users an opportunity to pause and consider their words before they post something.

BLOCK, REPORT OR MUTE

If someone is upsetting your child on Twitter, you can block and report them. Blocking stops them from messaging or following your child, while reporting an account alerts Twitter to investigate possible misuse. The 'mute' feature, meanwhile, keeps tweets from a specific account (or which include certain words) out of your child's timeline. The other user won't know that they've been muted.

BE CAREFUL WHO TO FOLLOW

As accounts are no longer being as rigorously verified under the 'blue tick' system, it's essential that young Twitter users understand what this means, in terms of people not necessarily being who they claim. Anyone who your child only knows online is *still* a stranger, regardless of how long they've been communicating for. Remind your child never to disclose personal information on social media.

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

Source: https://blog.twitter.com/common-thread/en/topics/stories/2022/how-twitter-is-nudging-users-healthier-conversations | https://blog.twitter.com/en_us/topics/product/2022/twitter-blue-update
https://blog.twitter.com/en_us/topics/company/2022/twitter-2-0-our-continued-commitment-to-the-public-conversation | https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2131&context=etd

What Parents & Carers Need to Know about WIZZ

AGE RESTRICTION 12+

12+ App Store
Teen Google Playstore

Wizz is a networking app which allows users to connect and chat with other people around the world. Its principle is similar to a dating platform: users have a profile with up to three photos, along with optional interests and hobbies tags. This allows other like-minded people to be recommended in searches. If a user likes what they see on someone's profile, they can initiate conversation through the instant message feature; otherwise they swipe on. The app *does* use age verification technology when an account is created and groups users by age.

WHAT ARE THE RISKS?

OVER-SHARING

Immediately after setting up an account, users start receiving friend requests (mainly from the opposite gender). For many young people, this will be exciting and a boost to their confidence. As young people tend to be more trusting online and may believe what others tell them, however, this can lull them into dropping their guard and revealing personal information to strangers.

CATFISHING AND PREDATORS

Wizz uses Yoti, a digital ID system, to verify users' age. The AI only detects approximate age, though – so an older person who *looks* younger could be grouped with teens (or vice versa). Also, profile pics on Wizz don't have to match the face of the person who did the initial age verification: it would be fairly easy to create a fake account using another person's photos with a made-up name and age.

EXPLICIT CONTENT

During our research, conversations on Wizz very quickly turned sexual. Users frequently suggested 'taking it to Snap' (Snapchat's disappearing image feature can make it conducive to sharing explicit selfies), connecting on other social media, swapping nude or semi-nude pictures, or holding sexual chats. These users created an impression of the platform being sleazy and unsafe for young people.

INTIMATE IMAGES

It's not unheard of for young people to be coaxed into sending suggestive images of themselves over apps of this kind. Given that Wizz connects users with strangers, who may not be honest about their real intentions, a teenager might conceivably be persuaded to share sexually suggestive selfies by someone who they believed they had a trusting relationship with.

NO PARENTAL CONTROLS

The app claims to provide a secure and inclusive environment, but our researcher couldn't find any parental controls or safety features in evidence. If you report another user for inappropriate behaviour, you are offered the option to block them – but there's no indication as to whether the block has actually been successful, and there was no follow-up contact from the developers.

SECRETS AND SUBSCRIPTIONS

Wizz sent our researcher occasional 'mystery' friend requests from a blurred-out profile. To discover the sender's identity, users can either watch a video (usually an ad for a game or app) or take out a monthly subscription. Cynics might suggest this could be a way to exploit young people's curiosity into making them pay for the app, and that the 'secret admirers' are bots rather than real people.

Advice for Parents & Carers

TALK IT OUT

If your child has downloaded Wizz, talk to them about why they like it and who've chatted with. Have they shared any personal details with this person or connected with them on other social media platforms? Refresh your child's memory of the various risks that can arise from engaging with strangers online and get them to consider using a similar app with more robust safety features.

BE SUPPORTIVE

When connecting with strangers on apps like Wizz, seemingly innocent chats can quickly progress to become sexually explicit and lead to nudes being sent. Make sure your child knows to come to you if they're uncomfortable about anything they've been sent or been asked to send. If they've already shared something that they now regret, reassure them that you'll support them no matter what.

EMPHASISE CAUTION

Young people are far more inclined to see the good in others; they often overlook the fact that scammers set up fake accounts on apps like this with the intention of getting money or personal data. Remind them that not everyone online is who they claim to be, how easy it is for someone to create a bogus profile, and why it's vital to think twice about sharing anything on networking apps.

KEEP THINGS TRANSPARENT

It might feel awkward, but regular chats about your child's online life can be beneficial. If they seem suddenly anxious or secretive around their phone or tablet, they may have something they need to get off their chest. You could also consider not allowing digital devices in their bedroom, especially overnight – that's when a lot of the riskier conversations on apps like Wizz tend to take place.

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

Source: https://play.google.com/store/apps/details?id=info.wizzapp&hl=en_GB&gl=US | https://www.met.police.uk/advice/advice-and-information/sexual-offences/sextortion/