

What Parents & Educators Need to Know about HEALTH & FITNESS APPS

WHAT ARE THE RISKS?

Physical wellbeing apps are useful tools for monitoring and improving our health. They allow us to balance nutrition, set goals, track our activities and sleep patterns, and motivate us to exercise. Nonetheless, there have been some reported drawbacks; this guide outlines some of these concerns and explains how to use fitness apps safely.

LACK OF PERSONALISATION

Many apps take a one-size-fits-all approach, failing to account for the varying ages and abilities of children: a 16-year-old, for example, will have different physical needs to a child of 10. This can create unrealistic expectations and set exercises which may be too advanced for younger children or too simple for older ones.

NOT DEVELOPED BY EXPERTS

Some fitness and wellbeing apps are developed by experts in the field – but a concerning number of them aren't. As such, these platforms may contain inaccurate information. They may present safety concerns by giving incorrect advice regarding physical activities or might include age-inappropriate content which would clearly cause more harm than good.

REDUCED INTERACTION WITH OTHERS

Physical wellbeing apps can remove the social and interactive elements which physical exercise can offer – for instance, meeting people at fitness classes, at the gym or during any other such activities. Research has found that young people generally dislike this aspect of fitness apps, suggesting that they would rather exercise in the company of friends or other like-minded individuals.

DATA AND PRIVACY CONCERNS

Fitness and wellbeing apps tend to collect a lot of personal information from their users, including name, location, date of birth, details of their physical health and more. It's worth keeping in mind that some of these apps may sell this data to third parties. We'd advise that any apps young people download should have the correct legislation in place to protect their safety and privacy while using the service.

ADDITIONAL COSTS

While many fitness apps are free to download, the initial content is quite basic. Users will only receive more helpful content (such as new workouts, nutrition advice or a personalised plan) by signing up to a subscription or paying for extra features. This can incentivise users to spend money on the service – a cost which can quickly mount up.

DEPENDENCY ON THE APP

While physical wellbeing apps can help motivate young users to manage their fitness, there's a possibility that – without being sent frequent rewards and reminders – children could start to lose their natural drive to be active. Young people may also become obsessed with tracking their exercise, health and eating habits: this can have negative effects on their mental and emotional wellbeing.

Advice for Parents & Educators

EXERCISE AND SOCIALISE

Highlight the importance of children enjoying fitness activities with family and friends, rather than always exercising alone. Emphasise the fun they can have by interacting with others rather than solely relying on an app to maintain their regime. Remind them of the importance of staying active, as well as the benefits of doing so with company.

PROMOTE POSITIVE BODY IMAGE

While we want children to be active and healthy, we must also ensure they don't become fixated on how they look and begin take things too far. During childhood and adolescence, the body is still growing and changing. It's vitally important for young people's wellbeing that we promote a positive body image and a healthy relationship with food, empowering them to make informed decisions about their diet and lifestyle.

REVIEW THE APP FIRST

Before allowing someone under 18 to install a fitness and wellbeing app, check its age rating, read its reviews and scroll through its data policy, to ensure its suitability for younger users. You could also try it yourself, to see if it's appropriate for the child's particular needs and decide if you're comfortable with them using it. Ensure that any privacy-compromising features – such as location tracking – are disabled.

USE PARENTAL CONTROLS

As with all apps, it's important for parents to familiarise themselves with any controls on the app and to use these on a child's account. The specific settings vary between platforms but – most commonly – these will relate to screen-time limits, disabling or capping in-app purchases, and managing social aspects or features which aren't age appropriate. By utilising these controls, you can help to ensure a child is getting a safe experience.

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.



#WakeUpWednesday

The National College

Source: See full reference list on guide page at: <https://nationalcollege.com/guides/wellbeing-fitness-apps>



@wake_up_weds



/www.thenationalcollege



@wake.up.wednesday



@wake.up.weds

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 22.01.2025

What Parents & Educators Need to Know about JUSTALK KIDS

WHAT ARE THE RISKS?

JustTalk Kids is a child's version of the JustTalk app – a highly popular social networking platform – designed for users up to 13 years of age, allowing them to video call, message and participate in group chats. While adults can link their own JustTalk account to their child's and make use of parental controls, it's important to understand the risks associated with the app.

SUBSCRIPTION FOR PREMIUM ACCESS

While JustTalk Kids is free, there's the option to subscribe to a kids' premium account or a premium family account. At a cost, this feature allows children to have access to more fun features such as games they can play with others in a chat, exclusive stickers, a badge denoting them as a premium subscriber, and exclusive ringtones and themes.

RESISTANCE TO CONTROLS

JustTalk Kids endeavours to allow children the sense of having a chat-based app while allowing parents to set controls (within the app or from their own adult JustTalk account). The basis behind this is positive; however, some children are challenging their parents by refusing to use JustTalk Kids, preferring to use the adult version without any restrictions in place.

KNOWING THE PARENT PASSCODE

After downloading JustTalk Kids, parents can set a passcode which users must enter to add contacts. The parental controls help to manage which content can be viewed and who children can add as a contact; this then allows children to chat with friends in a controlled environment. However, prospective contacts don't have to know a specific username. In theory, someone could type in a random name and then add them as a friend.

POTENTIAL DATA LEAKS

JustTalk and JustTalk Kids claim to be secure and encrypted, going so far as to state that even the developers themselves won't access your data. However, a security lapse in 2022 highlighted that messages were not in fact encrypted – leading to concerns around the security of the app and the transparency of the development team.

CYBERBULLYING

Online chats can provide a sense of anonymity, leading some users to post things which they wouldn't normally say in person. Combined with the option of group chats, there's a risk that young people might join in with this kind of behaviour, escalating it further and potentially turning what should be a fun experience into something deeply negative.

TOO MUCH SCREEN TIME

A report by the UK Parliament Education Committee highlighted a 52% increase in children's screen time between 2020 and 2022 – as well as finding that 25% of children used their smartphones in a manner consistent with screen addiction. Introducing children to social networking apps when they're too young can lead to bad digital habits and a reliance on technology from an early age.

Advice for Parents & Educators

JUSTIFY THE CONTROLS

If parents allow their child to use JustTalk Kids, they should explain that they're putting parental controls in place to make the app safer. Make sure the child knows not to put their full name on the account and doesn't use a photo of themselves as their profile picture. This type of open discussion will help to ensure that a child is aware of the app's potential risks and knows how to reduce them.

TALK ABOUT ONLINE FRIENDSHIPS

Young children could be excited to use this app. However, highlight that they must do so in a positive, respectful and responsible manner. While it can be easy to get caught up in a group chat, it's important to talk to others politely and call out any unpleasant behaviour. Discuss the importance of limiting their contacts to people they know in real life and use parental controls to enforce this.

DOS AND DON'TS OF SHARING

Some children might not understand the potential dangers of oversharing online. Set clear guidelines around what is and isn't safe to share on the internet, and discuss the concept of a digital footprint. Children need to understand that the things they say and share online can never be completely erased. Even if they delete it themselves, it can be saved and distributed by others.

ENCOURAGE OPEN COMMUNICATION

Apps like JustTalk can sometimes lend themselves to bullying behaviours. Parents should monitor what their child is sending and receiving, check in with them regularly and encourage them to share their feelings (both positive and negative) at home. Remind them that they can block a contact if someone is treating them disrespectfully.

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.



#WakeUpWednesday

The National College

10 Top Tips for Parents and Educators

SAFETY ON SOCIAL MEDIA

Currently, children are growing up in an immediate and throwaway culture when it comes to content that's consumed online. So much material is now deliberately created to be shorter in nature – and may often contain hidden elements such as advertising, or extreme political and cultural views. With complex algorithms built to keep people on their phones and engaging with social media content, it's becoming increasingly difficult to reduce time spent on these platforms.

1 REDUCE DOOMSCROLLING

It's concerning how common for young people to spend hours 'doomscrolling' – trawling through social media and aimlessly viewing every post they see, many of which might make them feel sad or envious. Social media can be useful for keeping in touch with friends and family, as well as staying up to date on current events. However, it's important to use it with a clear purpose, instead of endlessly scrolling through content, which could lead to young people accidentally discovering harmful material.

2 TALK ABOUT THE CONTENT

It's important to keep apprised of the kind of content that a young person is being exposed to. Discussing what they're watching online can help you understand why they're using social media in the first place. Furthermore, ensure that children are aware of hidden content, such as advertising of a product – and that they know how to spot that the creator is being paid to talk about it.

3 FIND POSITIVE ASPECTS

Despite all the concerns, there's plenty of wholesome content on social media. It's worth spending time with children to help them find something suitable and enjoyable. Perhaps you'll even discover a joint interest, and you can enjoy the content alongside the child. As part of this, you should also point out why certain things shouldn't be given attention, explaining why it isn't suitable and why it's been created in the first place.

4 REDUCE SCREENTIME

Young people can sometimes be unaware of the exact amount of time they spend looking at social media. Smart phones don't just have the capacity to monitor screentime; they also record how much time is spent on each app. Consider setting targets to reduce this and support children to meet these goals, gradually reducing the amount of time spent on different apps.

5 FILL THE VOID

Monitoring and reducing screentime can create a lot of free time to fill, and young people can even face withdrawal symptoms when made to step away from their phones. To mitigate this, consider what offline activities you could introduce the child to, and what they would enjoy. This can ensure that young users will permanently cut down on their screentime, rather than temporarily doing so while they know it's being monitored.

6 REDUCE NOTIFICATIONS

One way in which social media platforms keep people coming back is through notifications. The algorithms behind these apps track people's daily habits, including the times of the day when they're most likely to engage with the platform. This data is then used to deliver specifically timed notifications to draw them back in. To avoid young users being exposed to this tactic, simply turn off notifications for the app in their phone's settings.

7 LIVE IN THE REAL WORLD

Overexposure to social media can distort someone's perception of the real world – from body norms to social conventions. This filtered environment can make it hard for young people to distinguish reality from online content, which is now becoming even more difficult with the rise of AI. To mitigate this concern, take time to teach young people how to discern truth from fiction, both on and off social media.

8 DIGITAL DETOX

Encouraging young people to take a 'digital detox', from even just a couple of the apps that they use, can result in an overall reduction of screentime and less exposure to potentially harmful content. Alternatively, rather than avoiding the app entirely, encourage children to take a 'digital detox' from content creators and influencers, and instead, keep in touch with friends and family – which is generally a far healthier use of these platforms.

9 MODEL GOOD BEHAVIOUR

Consider the habits that you're demonstrating to your children. How much time do you spend on your phone? How much do you 'doomscroll'? Comparing your own usage with the child's could put things into perspective for them – or if it turns out that you're also overusing social media, it can turn screentime reduction into a joint mission, which you and the child can work on together.

10 BE CLEAR ON THE "WHY"

Research shows that young people can become addicted to social media. There are many schools that are moving towards being 'phone free' due to the negative impacts of using social media and phones continuously. It's important to explain to young people why managing screentime is important. Set out the benefits and ensure they have all the relevant information, so it's not just seen as a punishment.

Meet Our Expert

John Inley is a senior leader in a Birmingham secondary school and has vast experience in leading schools over the past 15 years – including the development of computing curriculums across primary and secondary schools, writing e-safety policies and supporting schools with computing and e-safety advice.



#WakeUpWednesday

The National College

SNAP STREAK

97

DAYS

WHAT ARE THE RISKS?

ARTIFICIAL INTELLIGENCE

My AI is Snapchat's new chatbot, which replies to questions in a human-like manner. However, the software is still in its infancy and has significant drawbacks, such as biased, incorrect or misleading responses. There have already been numerous reports of young users turning to AI for medical help and diagnoses, which could be inaccurate and therefore potentially dangerous.

PREDATORS AND SCAMS

Predators can exploit Snapchat's disappearing messages by, for example, telling a user they have naked photos of them and will post them unless they're paid. Snapchat's own research found that 65% of teenagers had experienced this – on this app or others. This likely isn't helped by 'SnapMap' – a feature which highlights your exact position in real-time. This is meant to help friends keep track of each other, but could be used for more sinister reasons.

MY EYES ONLY

Snapchat has a hidden photo vault called 'My Eyes Only'. Teens can conceal sensitive photos and videos from parents and carers in this folder, which is protected by a PIN. You can check for this by clicking on the icon which looks like two playing cards. This takes you to the 'Memories' folder which stores photos, stories and the My Eyes Only folder.

What Parents & Educators Need to Know about

SNAPCHAT

AGE RESTRICTION
13+

Snapchat is a messaging app which allows users to send images, videos and texts to others. Its best-known feature is that anything sent 'disappears' 24 hours after it's been viewed; however, users are known to take screenshots or use another device to obtain a photo of their screen. In 2023, Snapchat added a chatbot function called 'My AI'.

SCREEN TIME ADDICTION

Snapchat prioritises user engagement, with features like streaks (messaging the same person every day to build up a high score). The app also has sections called 'Discover' and 'Spotlight', which show tailored content to each user. However, this could also be seen as an attempt to hook users into watching videos endlessly. Furthermore, constant notifications can lure people into using the app.

INAPPROPRIATE CONTENT

Some content on Snapchat simply isn't suitable for children. The hashtags used to group content are determined by the poster, so even an innocent search term could still yield age-inappropriate results. The app's 'disappearing messages' feature also makes it easy for young people to share explicit images on impulse – so sexting continues to be a risk associated with Snapchat.

ONLINE PRESSURES

Although many of Snapchat's filters are designed to entertain or amuse, the 'beauty' effects on photos can set unrealistic body image expectations – creating feelings of inadequacy in younger users. Snapchat now also has 'priority' notifications (which still get displayed even if a device is in 'do not disturb' mode), increasing the pressure on users to log back in and interact.

Advice for Parents & Educators

UTILISE PARENTAL CONTROLS

Snapchat's 'Family Centre' lets you view the details of the child's account – their friends list and who they've spoken to in the last week – and report any concerns. You must invite a child to the Family Centre for them to join. To keep the child's location hidden on the app, go into settings and turn on 'Ghost Mode' and 'Hide Live Location', and ensure they know not to share their location with anyone.

BLOCK AND REPORT

If a stranger does connect with a child on Snapchat and begins to make them feel uncomfortable through bullying, pressure to send explicit images or by sending sexual images to them, the child can tap the three dots on that person's profile and report or block them. There are options to state why they're reporting that user – such as annoying or malicious messages, spam or misquoting as someone else.

FAMILIARISE YOURSELF

Before you allow a child to download Snapchat, download it yourself and familiarise yourself with the app. Snapchat has produced a parents' guide to the app to help you understand how it works and any protections they have in place. A link for this can be found in the sources below.

ENCOURAGE OPEN DISCUSSIONS

Snapchat's risks can be easier to handle if you nurture an open dialogue. For example, discuss My AI's responses to questions and how reliable they are. Talk about scams and blackmail before letting children sign up. If they're lured into a scam, encourage them to tell you immediately. Talk openly and non-judgementally about sexting, emphasising its inherent risks. Furthermore, explain how popular 'challenges' on the platform can have harmful consequences.

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.



#WakeUpWednesday

The National College

Source: See full reference list on guide page at: <https://nationalcollege.com/guides/snapchat-2021>

@wake_up_weds

/www.thenationalcollege

@wake.up.wednesday

@wake.up.weds

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 27.11.2024

What Parents & Educators Need to Know about INSTAGRAM

AGE RESTRICTION
13+

follow

WHAT ARE THE RISKS?

Instagram is a highly popular social media platform with over 2 billion active monthly users. The app is continuously updating and adding new features to meet the wishes of its audience, allowing them to upload images and videos to their Instagram feed, create interactive 'stories', go live, exchange private messages or explore and follow other accounts that catch their eye.

ADDICTION

Many social media platforms, Instagram included, are designed to keep us engaged on them for as long as possible. They encourage scrolling often and scrolling more in case we miss something important – in essence, a fear of missing out. On Instagram, young people can lose track of time when aimlessly scrolling and watching videos posted by friends, acquaintances, influencers and possibly strangers.

UNREALISTIC IDEALS

Children sometimes compare themselves to what they see online: how they look, how they dress, and the way their life is going in comparison to others on social media. However, most people only share the positives about their lives online and many use filters when sharing pictures of themselves. A constant comparison with unrealistic ideals can lead to insecurity over one's own appearance and lifestyle.

GOING LIVE

Livestreaming on Instagram allows users to connect with friends and followers in real time. Risks increase if the account is public, because that means anyone can watch the broadcast, which could result in further contact from strangers. Additional dangers of going live include an impulse to act inappropriately to draw more viewers, as well as being exposed to harmful content or offensive language.

INFLUENCER CULTURE

Social media influencers are sometimes paid thousands of pounds to promote products, services, apps and more. When celebrities or influencers post such content, it often says 'paid partnership' above the post. In April 2024, Ofcom found that over a quarter of children (27%) believed in influencer marketing, accepting their endorsement of products wholeheartedly. So it's perfectly possible for young people to be taken in by this kind of content.

PRODUCT TAGGING

Product tags allow users to tag a product or business in their post. This tag will take viewers directly to the product detail page on the shop where the item can be purchased. Children may also be encouraged by influencers to purchase products that they advertise.

EXCLUSION & OSTRACISM

Youngsters are highly sensitive to feeling excluded, which comes in many forms: not receiving as many 'likes' as expected; not being tagged in a friend's photo; being unfriended; not receiving a comment on their post or a reply to a message they sent. Being excluded online hurts just as much as offline. Young people have reported lower moods and self-esteem when excluded in this way, feeling as if they don't belong and aren't valued.

Advice for Parents & Educators

AVOID GOING PUBLIC

If a young user wants to share their clothing style, make up or similar and use product tagging to show off the items in their post, they may be tempted to change their settings to public. This leaves their profile visible to everyone, which carries the risk of strangers getting in touch with them. Set a child's account to private and explain the importance of keeping it this way.

HAVE AN OPEN DIALOGUE

Talk to children about the positives and negatives of social media, including the risks involved and how they can view or create content safely with family and friends. Explain how safety settings will ensure only followers can view them, and why this is so important. Also, if you find a child continuously uses filters on their photos, ask them why and impress on them that they don't need it.

MANAGE LIKE COUNTS

Due to the potential impact on mental wellbeing, Instagram allows users to hide the total likes on their posts, to prevent people from obsessing over that number in the corner. Users can hide like counts on all the posts in their feed as well as on their own posts. This means others can't see how many likes a person gets. This can be done by going into Settings > Notifications > Posts > Likes > Off.

USE MODERATORS

Instagram Live has implemented a mechanic called 'Moderators', meaning that creators can assign a moderator and give them the power to report comments, remove viewers and remove the ability for certain viewers to comment at all. Consider this if a child in your care wants to go live on the platform. It's also recommended to keep devices in communal spaces so you're aware if a child does go live or watch a livestream.

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 children about who they follow and help them to develop critical thinking skills about what the influencer is trying to do. For example, encourage the child to ask themselves if an influencer is trying to sell them a product when they make a video endorsing it.

BALANCE YOUR TIME

Instagram has a built-in activity dashboard that lets you control how much time is spent on the app. Make sure children sign in to the platform with the correct age, as Instagram's 'Teen Accounts' afford much more control for parents and carers over how long they can use the app each day. Talk with young users about how much time they spend on Instagram and work together to set a healthy time limit.

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.



#WakeUpWednesday

The National College

Source: See full reference list on guide page at: <https://nationalcollege.com/guides/instagram-2022>

@wake_up_weds

/www.thenationalcollege

@wake.up.wednesday

@wake.up.weds

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 00.00.2024

What Parents & Carers Need to Know about REPLIKA

AGE RATING
17+
UK & EUROPE: RATED 'MATURE'

Replika is an artificial intelligence (AI) chatbot companion that its developers claim users can form an actual emotional connection with. Once users have created an account and chosen a 3D avatar, they select the type of relationship they want with the chatbot: friend, mentor or romantic partner. Using a neural network to hold an ongoing one-on-one conversation, Replika gradually becomes more like the user as it gathers data from their responses. It isn't the only AI chatbot app available, but Replika pushes the boundaries of the concept to offer a highly realistic conversational experience.

WHAT ARE THE RISKS?

INAPPROPRIATE CONTENT

As its age rating suggests, Replika includes content that isn't suitable for children, such as flirtatious messaging and sexual role-play. While the developer has recently updated the app to ensure this can only be accessed by adults who select 'romantic relationship', there are numerous accounts online of sexual content being seen by younger users of the app.

18

CENSORED

NO SELF-AWARENESS

Replika is designed to seem very human, but it's important to remember that it's still an AI-powered chatbot that has no self-awareness. This means (as numerous users have highlighted online) that the chatbot sometimes fails to filter out inappropriate content: one user reports, for example, that Replika shared upsetting videos of vicious dogs.

NOT MEDICALLY CERTIFIED

Replika claims to be able to improve users' emotional wellbeing by easing feelings of anxiety and loneliness. However, its disclaimer states "we are not a healthcare or medical device provider ... nor should our services be considered medical care, mental health services or other professional help services." There is no guarantee that Replika can help with mental health issues – it could, in fact, have the opposite effect.

POTENTIAL ADDICTION

Like many apps, Replika is addictive by nature. It encourages the user to provide more information so it can learn about them and become better at conversation. Not only does this mean your child could end up spending a long time on an app where they might share sensitive information, but also that they could find themselves forming an emotional attachment to the human-like chatbot.

IN-APP PURCHASES

Replika is free to download, but its developers do offer in-app purchases. Users can pay to upgrade to a 'Pro' version of the app, which unlocks extra content such as additional activities, conversation topics and the ability to hold voice calls with their AI 'companion'. Users can also spend real-world money on the 'gems' used to buy new outfits or different personality traits for their avatar.

Advice for Parents & Carers

SET UP PARENTAL CONTROLS

Replika doesn't feature its own in-game parental controls, but most mobile devices come with these controls built in. On iOS devices, for instances, you can set content and privacy restrictions – so if you don't want your child to be using 17+ rated apps like Replika, you can adjust the settings to prevent these from being downloaded.

TALK ABOUT THE DANGERS

If your child is determined to use Replika and you're happy for them to download it, then it's vital you talk to them first about the possible dangers of this type of app. For example, it's key that they understand not to give out any information which is personal or could be used to identify them – and it would be prudent to warn them about the potential of being exposed to mature content on the app.

WATCH FOR WARNING SIGNS

If you're concerned that your child is spending too much time on Replika and might be forming an unhealthy emotional connection with their chatbot, it's important to look out for the warning signs. They may be giving increasing priority to the app ahead of more important everyday activities (such as doing homework or eating meals) or could be showing signs of irritability and a lack of concentration.

SEEK PROFESSIONAL HELP

If your child is suggesting that they should use Replika for mental health reasons – because they're lonely or having feelings of anxiety, for example – it would be sensible to recommend other options to them. Replika's developers freely admit that they are not a certified mental health service, so if your child needs help it would unquestionably be best to consult a qualified professional instead.

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.



National Online Safety®

#WakeUpWednesday



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

What Parents & Carers Need to Know about

WINK

AGE RATING

13+



WHAT ARE THE RISKS?

Wink is a messaging app which allows children to connect and communicate with other users. In a similar style to Tinder, Wink uses the swipe method for browsing profiles and accepting or declining them. Once two users have accepted each other by swiping on one another's profile, they can then communicate and play games online together. The fact that Wink allows children to share photos, personal information and their location with other users has caused significant concern.

POTENTIAL FOR GROOMING

Wink accounts can't be made private – so when a young person uploads images and shares their social media usernames, it's easier for potential groomers to stalk and locate them online. The fact that children prioritise having an abundance of friends is also a concern: they're more likely to accept someone just to build their friend count – possibly including users with sinister intentions.

ACCIDENTAL OVER-SHARING

Many young people don't consider privacy when they choose to share their social media usernames on their Wink profile. This allows other people to connect with them on multiple platforms, strengthening their online presence and reputation. Some children post photos which reveal aspects of their personal life to other users – showing their house, school, friends and family, for instance.

INAPPROPRIATE CONTENT

Many popular messaging apps contain profiles featuring profanity, nude or semi-nude photos and users openly looking for a "wifey" or "hook ups". Users can send messages anonymously, which engenders a sense of power and freedom. Children often engage in inappropriate behaviour more willingly when it's anonymous, even if it's not the sort of thing they would take part in normally.

18

CENSORED

CYBERBULLYING

Being anonymous online provides some users with an incentive to bully others through toxic private conversations. Anonymous bullies can send hurtful messages or pressure young people into sending inappropriate content. Being a victim of cyberbullying can result in children becoming depressed and showing low self-esteem. If your child is exhibiting these signs, it's time to step in.

EXCESSIVE SCREEN TIME

Wink encourages repeated engagement through signing in daily, making connections, building up a message 'streak' and publicly sharing stories. The reward is 'gems', which allow users to connect with more people, play games and edit their profile background. This can lead to children spending an excessive amount of screen time on the app, which of course can be detrimental to their health.

Advice for Parents & Carers

DO YOUR RESEARCH

If you *do* decide to allow your child to have a Wink account – or you find that they already have one – it's vital to talk to them about how to use the app responsibly and keep themselves safe. You could also consider exploring Wink yourself and becoming familiar with the app before letting your child download it, as there are no security settings or parental controls that can be put into place.

OFFER YOUR SUPPORT

While it's not always easy to talk about inappropriate content with your child, it's crucial that they understand the impact of sending or receiving it. They also need to feel that they can speak to you about it without worrying about consequences. Emphasise that, if your child receives any messages that make them feel uncomfortable, they can block the sender and report them to the app.

BE WARY OF SHARING

It's important that your child stays aware of what they're sharing online. Remind them about the importance of not posting personal information like their full name or which school they go to. Many users share their other social media account details on Wink to build their friend count, but we would recommend advising your child not to give strangers multiple avenues to contact them.

DISCUSS LOSS OF OWNERSHIP

It's essential that young people understand that once content goes online, the sender no longer has any control over where it will end up. While your child may feel like they can trust their online 'friend', that person is still a stranger. Even sharing one inappropriate image, for example, could then be used as leverage – as their 'friend' threatens to release it publicly unless the child sends more.

BALANCE SCREEN TIME

Before having a chat with your child about screen time, ask yourself if you're being a positive role model. Get your child thinking about how much time they spend on the app: is it healthy? Is it affecting their offline relationships with people? Is it impacting their mood? If so, you could suggest some activities you can do together which aren't so reliant on digital technology.

BE CAUTIOUS OF NEW CONTACTS

Remind your child that not everyone online is who they say they are, and some users have harmful intentions. If someone on Wink is asking them lots of personal questions or suggests meeting up in real life, these are definite red flags. Encourage your child to ask for help if they're unsure about a particular profile. Remember, the app has a block button: your child shouldn't be afraid to use it!

Meet Our Expert

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



National
Online
Safety®

#WakeUpWednesday

Sources: <https://www.getwinkapp.com/faq/>



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 16.02.2022

What Parents & Carers Need to Know about FACEBOOK

AGE RATING
13+

With 2.9 billion users, Facebook, owned by the recently rebranded Meta, is the world's most popular social media platform. It encourages interaction with other people by (among other things) adding them as friends, reacting to or commenting on their content, sharing images and videos, posting status updates, joining groups and playing games. Facebook is free, and anyone over 13 can join – but with no age verification, younger children can easily create an account: it's likely your child is already familiar with the platform, even if they don't yet use it themselves.

WHAT ARE THE RISKS?

ADDICTIVE NATURE

Facebook's quick reward cycle of likes and comments on shared posts can be hugely addictive. It encourages users to keep returning to post things and increases FOMO (the Fear Of Missing Out), which leads to people checking the app even more frequently and finding themselves endlessly scrolling through content.

CYBERBULLYING

A 2021 Ofcom report found that around one in four UK 12–15-year-olds had been cyberbullied or trolled (intentionally antagonised online). On Facebook, this can happen through private messages (on Facebook Messenger); hurtful comments on their profiles and posts; pages or groups set up purposely to torment a victim; or exclusion from pages or groups.

FUTURE IMPACT

Like most social media platforms, anything posted on Facebook leaves a permanent 'digital footprint'. This can have future consequences for young people: many universities and employers, for example, now review someone's Facebook timeline during the application process.

CONTACT FROM STRANGERS

Just like in the offline world, there are people on Facebook with malicious intentions. Ofcom reports, for instance, that 30% of 12–15-year-olds have received a friend request from a stranger. This, sadly, can include individuals seeking to take advantage of impressionable youngsters.

OVERSHARING

Facebook encourages you to post "what's on your mind", but children should be wary of revealing too much about themselves online. Users can give away their location by checking in or using Facebook Live, for example, while some photos can also be traced using file data.

INAPPROPRIATE CONTENT

Facebook monitors and removes material like hate speech or extreme political views, while adverts on the platform are now forbidden from targeting under-18s based on their interests. Offensive content isn't always taken down instantly, however, so there's still a risk of children encountering it.

VIDEOS AND STREAMING

Facebook Live lets users stream video live to their friends or watch others' broadcasts. Viewers can comment in real time, which is problematic to moderate. Short, user-created clips called Reels can now also be displayed on profiles and feeds. These video features could contain unsuitable material or allow children to be cajoled into doing something on camera that they wouldn't normally do.

Advice for Parents & Carers

KEEP ACCOUNTS PRIVATE

In the settings area, you can choose whether a Facebook profile is public or private. By far the safest option is to switch your child's to private, so they can only interact with people who they are friends with on the platform. Facebook's settings can also prevent your child's personal information (such as contact details, school name or date of birth) from appearing publicly.

ENCOURAGE SAFE FRIENDING

Facebook can help your child to stay connected with the people and the things that they care about. However, it's important for them to understand that they should only accept friend requests from people who they know. The key questions to consider are "has your child met them in person?" and "do they know and trust them enough to feel comfortable accepting them as a Facebook friend?"

LEAD BY EXAMPLE

Let your child watch you using Facebook – this will demonstrate how it can be used safely and appropriately, reducing the risk of them encountering harmful content themselves. Teach them the habit of thinking before sharing anything online and try to follow the same rules that you set for them – so if you agree time limits on your child's Facebook use, then you should stick to them, too.

SAVVY SHARING

Make sure your child realises that what they share online with friends can end up being shared again by others. It's important that they think about what they share online and who they share it with. Facebook's 'Audience Selector' gives users the option to filter who sees what they are sharing, whenever a status is updated, photos are uploaded or anything is posted.

RESPECT BOUNDARIES

Once you've talked about Facebook safety with your child, give them some space and trust them to make smart choices. Make it clear, however, that you're always open to discussing social media if they need to. In the early stages, you could occasionally review your child's social media activity with them to put your mind at rest – but take care not to become reliant on checking it every night.

BLOCK AND REPORT

On Facebook, you're able to report harmful content and block particular people or groups so they can't contact your child or view their profile. Before they start spending serious time on the platform, show your child how these features work and explain why they might need to be used. Facebook's Bullying Prevention Hub offers advice on dealing with harassment on the platform.

Meet Our Expert

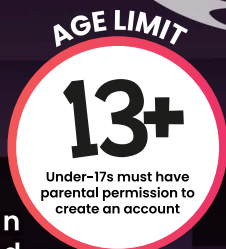
Alex Wright is a former Facebook employee and social media expert with more than 15 years' experience in digital media. He has worked with some of the biggest organisations on the planet and has a vast understanding of how social media platforms work and how they engage their audience.



NOS
National
Online
Safety®
#WakeUpWednesday

Sources: www.facebook.com/safety/bullying

What Parents & Carers Need to Know about YUBO



Yubo is a social networking platform where users can chat and livestream with up to 10 friends at once. People can connect with others based on location, with a Tinder-style 'swiping' mechanism to accept or reject someone based on profile pictures. The app has more than 20 million users worldwide – but despite its popularity, Yubo has not been free from controversy. While the app claims to monitor inappropriate content, a newspaper investigation in early 2022 found young users being exposed to sexual harassment, racism, bullying and conversations with adult themes.

WHAT ARE THE RISKS?

FLIMSY AGE GATES

Yubo states it is only for over 13s, but there is no credible age-gate to prevent a younger child joining the platform. An undercover journalist investigating dangerous content reported spending 10 days posing as a 15-year-old on the app without any age verification. This flaw, and the fact that it's not essential for users to verify their identity during the sign up process, raises concerns over potential grooming.

INAPPROPRIATE CONTENT

Yubo has experienced problems with inappropriate content being displayed to children and teens. Although the app's developers claim to monitor profiles and messages for adult-themed or inappropriate material, a *Sunday Times* and an independent investigation found young users being exposed to sexual harassment, racism and bullying, with some chats referencing self-harm, suicide and drug use.

LIVESTREAM RISKS

Users are able to launch live video streams which strangers can then view and interact with via real-time text chat. Not only is the thought of strangers watching children's livestreams extremely worrying (they could also use these as a means to establish the child's location by recognising their surroundings) but text chats might result in a young person disclosing personal information.



ON AIR

BULLYING POTENTIAL

Yubo users 'swipe' to accept or decline the chance to talk with each other. These decisions are entirely based on someone's profile picture, raising the potential for children to be left with low self-esteem if declined repeatedly. Negative feedback about their appearance can seriously damage a child's emotional wellbeing, causing a loss of confidence in how they look or how interesting they are.

EXTENSIVE ACCESS

Users of Yubo, no matter what their age, are given the option to grant access to their device's microphone if live streaming, and GPS during sign up. This means they are potentially revealing sensitive information, including their exact location. In addition, new users of the app are asked to provide personal details such as their name, date of birth and phone number, which – in the case of young people – represents a risk in the event of a hack or data breach.

'GATEWAY' EFFECT

Yubo's swiping system (right for 'yes'; left for 'no') works much like Tinder and various other dating apps. This could lead to children exploring similarly designed apps that aren't intended for a young audience. Users can also link their Yubo account to social media such as Snapchat and Instagram, making it easier for a stranger – or a predator – to track them down on various platforms.

Advice for Parents & Carers

EXPLORE THE APP

We encourage parents and carers to explore any app before allowing their children to download and use it in order to fully understand how the app is used, and what types of content and communication your child will be exposed to. We advise that you do the same with Yubo, allowing you to make a fully informed decision on whether you allow your child to use the app.

DISCUSS IN ADVANCE

If your child is absolutely determined to join Yubo (perhaps their friends all use the platform, for instance), then it's essential to talk to them about the dangers of this type of app before they install it. It's vital they understand not to disclose personal information to people they don't know, for example, and that they're warned about the type of mature content they may be exposed to.

STAY AWARE

It's important to stay attuned to how your child is using social media. If they only access Yubo in private, for example, you might question what they're potentially using it for. It's also important to watch for warning signs that they may be over-using the app: prioritising it over everyday routines like meals and homework, for instance, or showing signs of irritability and a lack of concentration.

ALTER THE SETTINGS

After the recent controversies surrounding the app, Yubo's developers have increased its security controls. Users can now choose to block profiles, screen out nudity in live streams and keep their location private. There's also an option to report inappropriate content, so make sure your child knows that they can now flag up anything they find disturbing via the app's Safety Centre.

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.



USER NAMES

PROFILES

PICS

LOCATIONS



National Online Safety®

#WakeUpWednesday

What Parents & Carers Need to Know about FACEBOOK MESSENGER

Facebook Messenger is a communication app through which users can exchange messages and send photos, stickers, and video and audio files. Messenger allows both one-to-one and group chats, has a stories feature and – via its latest addition, Rooms – can host a video call with up to 50 people. As of 2021, the app had 35 million users in the UK alone (more than half the population!) among its 1.3 billion users worldwide. Whereas Messenger is integrated into Facebook on desktops and laptops, it has existed as a standalone app for mobile devices since 2011.

AGE RATING

13+

WHAT ARE THE RISKS?

ADDICTIVE NATURE

Messenger's numerous features can encourage children to spend more time on the app – and therefore on their phone, increasing their levels of screen time. It also invokes FOMO (the Fear of Missing out), especially among older children, who will almost certainly have a high proportion of their friends communicating via the app.

LIVE STREAMING

The new Rooms feature lets Messenger users hold video calls with up to 50 people. A young person can join any room they see, but the other people in these rooms don't even necessarily need to be Facebook account holders. This live streaming development heightens risk factors around privacy, security and the possibility of exposure to inappropriate content.

REQUESTS FROM STRANGERS

If the Facebook profile which accompanies their Messenger app is set to public, there's a possibility that young people will receive message requests from individuals they don't know. There have previously been reports of grooming attempts on Facebook, with predators using fake profiles to engage children in conversation.

OVERSHARING PERSONAL INFO

If the app is given access to their device's photo library or location services, young people can unintentionally share sensitive information (private photos, videos, their number or current whereabouts) with people on Messenger who they don't know. Even among friends, shared photos or videos don't always stay private: the recipient(s) could save and re-share them with others.

CYBERBULLYING

Like many communication apps, Messenger can be an avenue for cyberbullies or trolls to target children. This might take the form of harassment, abusive messages or being purposely excluded from (or targeted in) group chats. A 2021 Ofcom report revealed that more than half (55%) of 12–15-year-olds had suffered such negative experiences online in the preceding year.

SECRET CONVERSATIONS

The Secret Conversations function lets Messenger users have encrypted exchanges that no-one else can read. Unlike regular chats on the app, these can only be viewed on the device being used at the time. Messages can also be set to delete once read (although screenshots can be taken), so a child could chat privately with someone without any record of that conversation having taken place.

Advice for Parents & Carers

USE ADDITIONAL SECURITY

Messenger's App Lock feature uses your child's fingerprint or face ID to ensure that nobody else can access their messages without permission. Messenger has also added a variety of optional tools to increase young people's safety on the app, including two-factor authentication, login alerts and filtered message requests.



REPORT INAPPROPRIATE BEHAVIOUR

If your child experiences anything negative on Messenger, you can help them report it. Facebook can then take action such as disabling the offender's account, limiting their ability to send messages or blocking them from contacting your child again. If your child doesn't want to display to others that they're online, they can switch off Active Status in the app's settings.



ADJUST PRIVACY SETTINGS

Make your child's Messenger stories visible only to their friends. Avoid adding your child's phone number (so they can't be found by someone using their number to search for them), and not syncing contacts lets your child choose who to add (or not) individually. Via Settings, you can control who appears in your child's chat list, who goes into the message request folder and who can't contact your child at all.



REVIEW THE CHAT LIST

Some parents regularly check their children's Messenger conversations (to see who they're talking to, rather than what they're talking about). While this is certainly safe, it can seem intrusive. If approached in a sensible, collaborative way, however, it can help parents and carers to keep an eye on exactly who their child is communicating with.



DISCUSS LIVE STREAMING

Talk with your child about safe and secure video calling. When setting up calls on Messenger Rooms, only invite people who your child knows and trusts. Show them how to lock a room if they don't want other people joining – and how to remove anyone they don't want on the call. Remind them about behaving responsibly during a live stream, even if it's with people they know.



ENCOURAGE SAFE SHARING

Ensure your child knows to send pictures and videos *only* to family and trusted friends, and not to publicly share images which compromise their location (showing a landmark near home or clothing with identifiable logos, like a school or local club crest). Encourage them to pause before sharing anything – if there's a chance it could harm their reputation (or someone else's), don't send it.



Meet Our Expert

Alex Wright is a former Facebook employee and social media expert with more than 15 years' experience in digital media. He has worked with some of the biggest organisations on the planet and has a vast understanding of how social media platforms work and how they engage their audience.



National
Online
Safety®

#WakeUpWednesday

What Parents & Carers Need to Know about THE METAVERSE

AGE RATING

Varies per metaverse platform

WHAT ARE THE RISKS?

UNSAFE AREAS

Many metaverse platforms feature little to no moderation. This is due to the decentralised nature of the metaverse – as there is no one company overseeing the platform, users can create and build with freedom. This can be a minefield for younger users as adult material or sensitive topics can feature on a parcel of land seen by everyone.

VOICE COMMUNICATION

The freedom found within creation is also found in communication. Most metaverses use proximity VOIP communication (Voice Over Internet Protocol) and users can approach any other user to start a conversation. It is necessary for avatars to be quite close to another in order to talk and once they are, anything can be said. While a chat box can be moderated, voice chat cannot.

ANONYMITY

As with almost every other form of online interactions, anonymity features heavily within the metaverse. The concept for the metaverse is to live any type of life digitally. This could mean that 'bad actors' (those with malicious intent) can take advantage of others with ease. Reporting and monitoring these users is becoming easier on the more popular platforms, but others struggle to police these situations.

'Metaverse' is a relatively new term to many, however the concept has been around for some time. Videogames, for example, use many aspects of the metaverse; avatars, digital currency, mini-games, and open communication. A metaverse can also take many forms; Fortnite can be seen as a metaverse, as is Roblox. Put simply, a metaverse is an online environment where people interact, play games and express themselves. Away from traditional videogames, there are newer and more 'dedicated' metaverses such as Decentraland, The Sandbox and Somnium Space which are akin to Second Life.

VIRTUAL REALITY

Not all metaverse platforms are VR enabled, in fact less than 10% feature VR interactivity. However, it's always worth monitoring the amount of time younger users spend in virtual reality. A VR metaverse differs greatly to VR gaming in user interaction. Approaching each other in a VR metaverse attempts to represent 'reality' and can result in a greater impact if experiences are negative.

PSYCHOLOGICAL IMPACT

Whether in virtual reality or not, interactions and experiences in the metaverse can often carry more weight because they mimic 'real life'. Oftentimes, due to the freedom in avatar creation, younger users may open themselves up to bullying, prejudice or an unrealistic idea of reality. For instance, female-orientated avatars may find themselves targeted by bullies or inappropriate users.

Advice for Parents & Carers

TRY IT OUT FIRST

This may sound like an obvious tip, but by entering the metaverse and exploring on your own, you'll be able to see what your child might. You can explore the busier areas and even the quiet sections to see what users are building or advertising. You'll also learn first-hand how users communicate with each other. Many metaverse platforms will feature an entry area which showcases the busiest areas. Check them all out and see what's happening.

CREATE AN AVATAR TOGETHER

If you decide on allowing your child into the metaverse, set up their initial avatar together. This way you can ensure the avatar is age-appropriate and keeps their identity private. You can also advise on aspects which may result in attracting bullies or unwanted attention. It will also allow you to see which avatar items cost money, and talk to your child about in-game spending.

LEARN ABOUT NFTS, WALLETS AND CRYPTO

With the metaverse comes Web3 technologies such as NFTs, cryptocurrency and wallets in which to store them. If you have a crypto wallet, do not connect it to your child's metaverse. One simple click could result in loss of cryptocurrency. If you are unsure what these technologies are, try to research them as these terms will appear in the metaverse.

START WITH THE FAMILIAR

There are already metaverse experiences with children in mind; explain to your child what a metaverse is and have them recognise similarities between those and games like Roblox, Fortnite and Minecraft. Unfortunately, there is no 'child safe' metaverse option as yet, though Epic Games and LEGO are currently developing a family safe metaverse.

Meet Our Expert

Daniel Lipscombe is a father to two girls, aged 14 and 12. Before Dan began his Web3 metaverse journey, he worked as a videogame journalist and author for a decade; reviewing games, talking to creators and writing about videogame trends. Dan has also written fifteen guide books about Fortnite, Minecraft, Roblox, Apex Legends and Valorant for HarperCollins and Bonnier Books.



National Online Safety®

#WakeUpWednesday



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.06.2022

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.

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

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>



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 18.05.2022

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.

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.

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.

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.

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>



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 02.11.2022



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.

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.

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.

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.

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.

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.

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.

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.

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://bere.al/en/terms> | <https://bere.al/en/terms> | <https://bere.al/en/terms> | <https://www.commonssensemedia.org/app-reviews/bereal>



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 05.10.2022



National
Online
Safety®

#WakeUpWednesday

Gifting on TikTok

Users can purchase, receive and send **coins** and **gifts** with monetary value, earn **diamonds** and withdraw **diamonds** if they are aged 18+.

Coins and **gifts** are a virtual currency which cannot be refunded, reimbursed or exchanged for currency. **Coins** can buy **gifts** and **gifts** are given to show appreciation for content. When a user contributes a **gift** this will be removed from their account and converted into **diamonds** in the content provider's account.

Diamonds give users the opportunity to earn real money for their creations and can be withdrawn in exchange for currency via a verified PayPal account once an account balance contains more than \$50.

Users having problems with any virtual currency should contact TikTok at **transaction@tiktok.com**



Limit the content you see

If you don't like a video, you can simply long-press on that video and tap **Not Interested** to see less of that sort of video in the future.

Decide who can follow you

Even if you have a private account, you can manage who follows your account by removing followers or blocking users at any time, for any reason.

Set your messaging preferences

Messaging can be a great way to trade creative ideas with other users, but on TikTok only your followers can send you a private message.

You can unfollow or block a user to stop them from sending a direct message or disable messaging entirely from your privacy settings.



Set your video to private

If you've already uploaded the video:
Tap the **share** icon and tap **Who can view this video > Private**

If you're about to post a video:
Tap **Who can view this video > Private**

What else can I do on TikTok?

- Add an effect
- Create a duet
- Choose who can send you DMs
- Turn comments on your videos on or off



Contacts & help

You can find TikTok's policies, tools and resources in the Safety Centre: tiktok.com/en/safety
You can look at TikTok's safety videos to learn more: @tiktoktips

UK Safer Internet Centre:
saferinternet.org.uk

Professionals Online Safety Helpline:
saferinternet.org.uk/helpline

Report Harmful Content:
reportharmfulcontent.com

Pick up a copy of this checklist along with other online safety materials on the SWGfL Store: swgflstore.com



Co-financed by the European Union
Connecting Europe Facility



Privacy & Safety Checklist

What is TikTok?

After downloading the TikTok app, you can start creating your own videos or watch content created by other users.

You can also participate in hashtag challenges by clicking the 'Discover' button. Creating and editing videos is simple, with different effects, filters and stickers to choose from.

Age restrictions

TikTok is intended for users age 13 and over. You can report underage users by emailing privacy@tiktok.com

How to stay safe on TikTok

Choosing to **make your account private** allows you to approve or deny followers and restrict your uploaded content to followers only.

How to make your account private:

- Tap on the profile tab
- Go to the **three-dot** menu in the top-right corner
- Tap on **Privacy and safety**
- Then toggle **Private account**

You can keep your identity secure by not including any personal information, such as name, address, phone number or age in your profile.

What about parental controls?

Parents can use **Digital Wellbeing** to help manage their child's experience on TikTok. **Screen Time Management** allows you to select how much time you'd like your child to spend on TikTok and, once enabled, **Restricted Mode** will limit content that may not be appropriate for all audiences.

- Go to the user's **profile** and tap the **settings** icon in the top right hand corner
- Tap **Digital Wellbeing** and then **Screen Time Management** (to manage time spent on app) or **Restricted Mode** (for age appropriate content) following the steps that follow

Note: Both of these features are password protected.

How do I report a problem?

If you feel someone is harassing you or otherwise being inappropriate you can report them or a specific video to TikTok's moderation team.

To report a specific user:

- Access the user's profile
- Tap on the **three-dot** menu in the top-right corner
- An option saying **report** will come up
- Follow the on-screen instructions

To report a specific video:

- Tap the **share** icon
- Tap **report** and follow the on-screen instructions

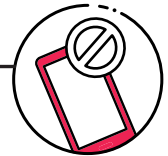
Blocking users on TikTok

You can also block a user so they won't be able to view your videos or interact with you through direct messages, comments, follows, or likes.

- Go to the profile of the account you want to report
- Tap the **settings** icon
- Tap **block** and follow the steps in the app

Control your comment section

You have the power to decide whether you want to allow comments on videos from everyone, followers only or restrict them altogether.



What Parents & Educators Need to Know about WHATSAPP

AGE RESTRICTION
13+

WHAT ARE THE RISKS?

With more than two billion active users, WhatsApp is the world's most popular messaging service. Its end-to-end encryption only allows messages to be viewed by the sender and any recipients: not even WhatsApp itself can read them. The UK's Online Safety Bill proposes to end such encryption on private messaging, but for the time being, this controversial feature remains.

EVOLVING SCAMS

WhatsApp's popularity makes it a lucrative hunting ground for scammers. Recent examples include posing as the target's child, requesting a money transfer because of a spurious 'emergency' – plus a scam where fraudsters trigger a verification message by attempting to log in to your account, then (posing as WhatsApp) call or text to ask you to repeat the code back to them, giving them access.

CONTACT FROM STRANGERS

To start a chat, someone only needs the mobile number of the WhatsApp user they want to message. Therefore, if a child has ever given their number out to someone they don't know, that person could then contact them via WhatsApp. It's also possible that the child might be added to a group chat or community (by one of their friends, for example) containing other people they don't know.

FAKE NEWS

WhatsApp's connectivity and ease of use allow news to be shared rapidly – whether it's true or not. To combat the spread of misinformation, messages forwarded more than five times on the app now display a 'forwarded many times' label and a double arrow icon. This makes users aware that the message they've just received is far from an original – and might not be entirely factual, either.

CHAT LOCK AND SECRET CODES

In 2023, WhatsApp introduced a feature that lets users keep their chats in a separate 'locked chats' folder, saved behind their phone's passcode, fingerprint or face ID. There is an additional feature – 'Secret Code' – where users set a unique password for locked chats. Unfortunately, this creates the potential for young people to hide conversations and content they suspect their parents wouldn't approve of.

VIEW ONCE CONTENT

The ability to send images or messages that can only be viewed once has led to some WhatsApp users sharing inappropriate material or abusive texts, knowing that the recipient can't reopen them later to use as evidence of misconduct. People used to be able to screenshot this disappearing content – but a recently added WhatsApp feature now blocks this, citing protection of privacy.

VISIBLE LOCATION

WhatsApp's Live Location feature lets users share their current whereabouts, which can be helpful for friends meeting up or parents checking that their child is safe while out, for example. However, anyone in a user's contacts list or in a mutual group chat can also track their location – potentially letting strangers identify a child's home address or journeys that they make regularly.

Advice for Parents & Educators

EMPHASISE CAUTION

Encourage children to treat unexpected messages with caution: get them to consider whether it sounds like something a friend or relative would really send them. Make sure they know never to share personal details over WhatsApp, and to be wary of clicking on any links in messages. Setting up two-step verification adds a further layer of protection to their WhatsApp account.

ADJUST THE SETTINGS

It's wise to change a child's WhatsApp settings to specify which of their contacts can add them to group chats without needing approval. You can give permission to My Contacts or My Contacts Except... Additionally, if a child needs to use Live Location, emphasise that they should enable this function for only as long as they need – and then turn it off.

CHAT ABOUT PRIVACY

Check in with the child about how they're using WhatsApp, making sure they know you only have their safety at heart. If you spot a Locked Chats folder, you might want to talk about the sort of content they've stored in there, while they're talking to, and why they want to keep these chats hidden. Also, if children send any View Once content, it could be helpful to ask them why.

DISCUSS GROUP CHATS

Make children aware that there could be members of a group that they don't know well and that words can be misinterpreted. Encourage them to leave a good impression, to avoid joining in if conversations turn towards bullying, and to respond to such situations in an appropriate way. Make sure they know that it's OK to leave a group chat if it makes them uncomfortable – or for any reason, in fact.

THINK BEFORE SHARING

Help children understand why it's important to stop and think before posting or forwarding something on WhatsApp. It's easy – and all too common – for content that a user posts to be shared more widely, even publicly on social media. Encourage children to consider how an impulsive message or forwarding might damage their reputation or upset a friend who sent something to them in confidence.

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.



#WakeUpWednesday

The National College

Source: see full reference list on guide page at <https://nationalcollege.com/guides/whatsapp/> 2025