At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one app of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know About WHATSAPP

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

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

'Prize' Scams

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

Enabling Fake News

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

Connections with Strangers

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

Ephemeral Messaging

By enabling the 'disappearing messages' option in a chat, users can send messages that will vanish from WhatsApp after seven days. Parents may want to take note of this new feature, which makes monitoring what children are talking about on the app problematic. Equally, if someone sends your child an inappropriate message, once it has disappeared there is no way to prove any wrongdoing.

'Only Admins' and Cyberbullying

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

Live Location Sharing

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

Advice for Parents & Carers

Report Potential Scams

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

Create a Safe Profile

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

Use Location Features Sparingly

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

Explain about Blocking

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

Leave a Group

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

Delete Accidental Messages

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

Fact-Check Messages

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

Meet Our Expert

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

National Online Safety®

#WakeUpWednesday

SOURCES: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/#:~:text=As%20of%20March%202020%2C%20WhatsApp,U.S.%20dollars%20in%20February%202014., https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/, https://www.whatsapp.com/?lang=en, https://en.wikipedia.org/wiki/Indian_WhatsApp_lynchings, https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-update-latest-india-hoaxes-forward-messages-app-download-a8456011.html, https://www.bbc.co.uk/news/technology-52441202

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: 10.03.2021

At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one app of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know About SIGNAL

12+ App Store Rating

Signal is a multimedia messaging service (previously known as TextSecure) which provides secure chats between users. It is encrypted, so any intercepted communication cannot be read by attackers. Users can send one-to-one messages or set up group chats. The service is free, has no adverts and doesn't track users' location like many other messaging platforms. The app experienced a popularity boom in early 2021 as large numbers of users left WhatsApp over perceived privacy issues.

Disappearing Messages

Messages on Signal can be set to disappear (from both the sender and the recipient's devices) a specified time after they are first opened – potentially as little as five seconds. So it is difficult to monitor the app and see what your child is talking about. Should someone behave inappropriately towards them, unless they record evidence instantly there is no way to prove what has happened – making it difficult to take the proper action.

Risk of Screengrabs

Because messages can be set to disappear on Signal, some young people assume that nobody else will ever see them and let their guard down as a result. But a recipient could still capture a screenshot of your child's message before it vanishes from their device. This screengrab – which might be of something inappropriate or deeply personal – can then be shared with others or even made public on the internet.

False Sense of Security

The feeling of total privacy and security within the app can make young people feel like they are invulnerable – and possibly that they could get away with behaving in ways they normally wouldn't. This behaviour could range from the harmful (such as participating in cyber bullying or sharing age-inappropriate images or videos) to the extremely dangerous: perhaps chatting to strangers, who might potentially be predators.

Vulnerability to Hackers

Like virtually any piece of software, Signal has been shown to have flaws in its security. One hacker was able to make a call to a target device using the app and could then listen in on the victim through their phone – without needing them to even answer the call. Afterwards, the hacked user was completely unaware that the eavesdropping had taken place.

Advice for Parents & Carers

Gather Any Evidence Quickly

If your children are old enough to use Signal, they will likely already know how to take a quick screenshot on their phone. It's best to confirm this with them, however, because if they're sent something inappropriate or offensive, they will only have a very short opportunity to screenshot it as evidence of misconduct before the message disappears. Once they've captured the screenshot, they should then come to you or another trusted adult.

Talk about Online Bullying

Before your child downloads Signal, have an open discussion about the potential risks of this app and others like it. Ensure your child is aware of the possibility of bullying or hurtful messages on such platforms. They should understand that the app makers themselves do not help with investigating incidents – and that it may be difficult to prove someone has done something to upset them.

Think before Sending

The messages a young person sends on Signal don't last forever, but the effects of those messages very well might – for your child and for others. You could suggest to your child that, if they're unsure whether to send a particular message, they should ask themselves if they would be comfortable showing the content to you. And if they wouldn't, should they really be sending it at all?

Stay Updated

It's wise to make sure your child knows how to keep their software up to date by downloading the latest version. Developers will often release software updates that (as well as occasionally adding new features or improving functionality, etc.) help to fix any security flaws and stop hackers from exploiting possible weak points in the app.

Consider Online Reputation

Talk to your child about the implications if a message they sent was made public without their consent. Remind them that once an image (for example) is out there, there's no way to control what happens to it or erase every single copy. It's a good way to get young people to start considering how their digital footprint might have repercussions on their future prospects.

Meet Our Expert

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

National Online Safety®

#WakeUpWednesday

SOURCES: https://smartsocial.com/signal-app/, https://www.signal.org

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: 03.03.2021