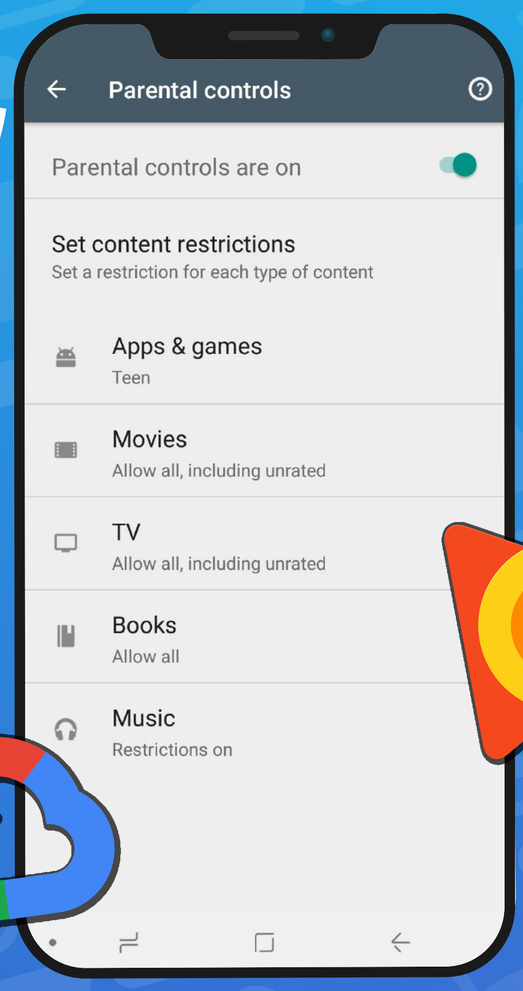
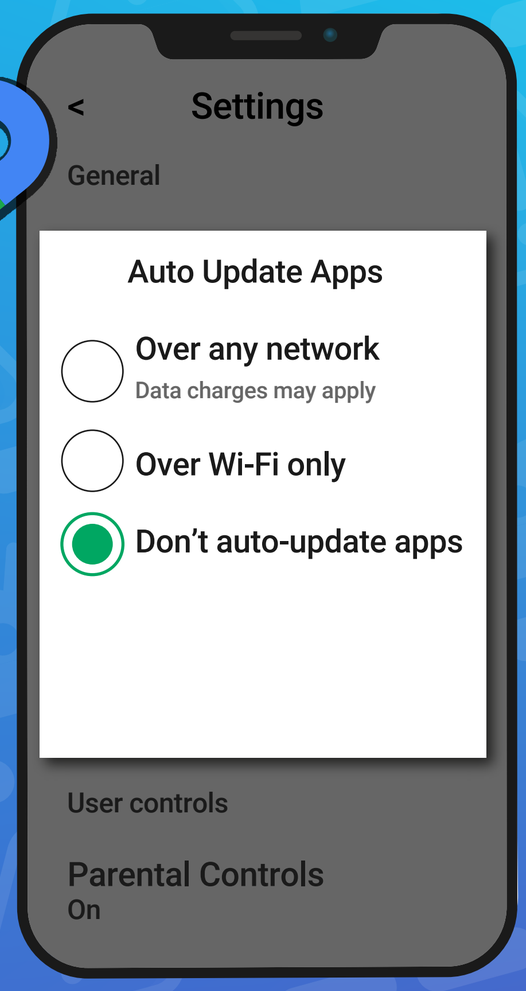
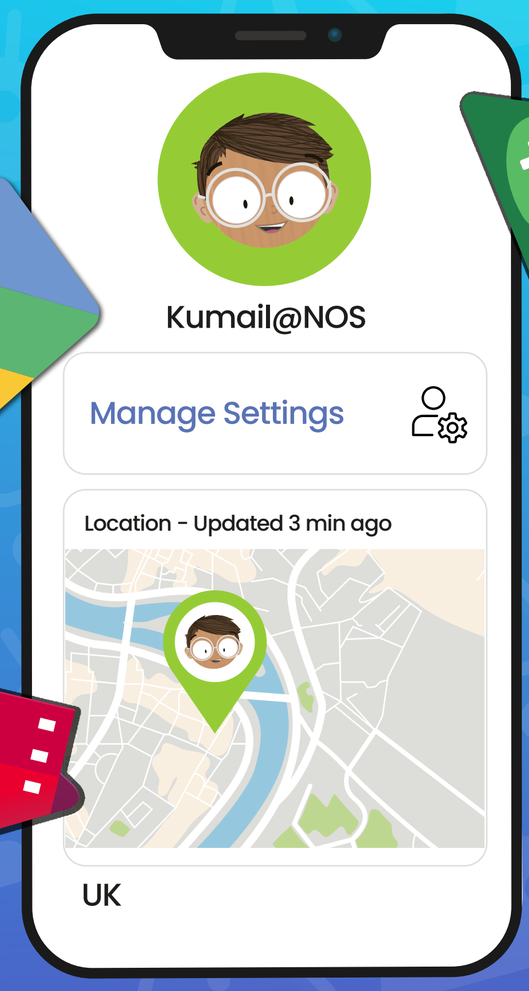
How to Set up PARENTAL CONTROLS for APPS

Android Phone

On Android phones, restricting access to particular apps usually requires going onto Google Play. From there, it's fairly easy to navigate your way through the settings to manage the parental controls and authentications relating to any apps on the device. These features can prevent your child from downloading or buying anything unsuitable for their age. Updated versions of apps or games that your child has already installed may occasionally contain something inappropriate, so we've explained how to stop those, too.







How to Block App Downloads (This Also Disables In-app Purchases):

1. Open Google Play Store
2. Tap the profile icon in the top right
3. Tap Settings
4. Scroll down to the Family section and tap Parental controls
5. Toggle 'Parental controls are off' to 'Parental controls are on'
6. Create a PIN and tap OK
7. Confirm your PIN and tap OK again
8. Tap Apps & Games
9. Set the age limit you wish to set
10. Tap Save to apply your changes

How to Stop Auto-updates

1. Open Google Play Store
2. Tap the profile icon in the top right
3. Tap Settings
4. Tap Auto-Update Apps
5. Select 'Don't auto-update apps' and then tap Done

Restricting Apps Through Google Family Link

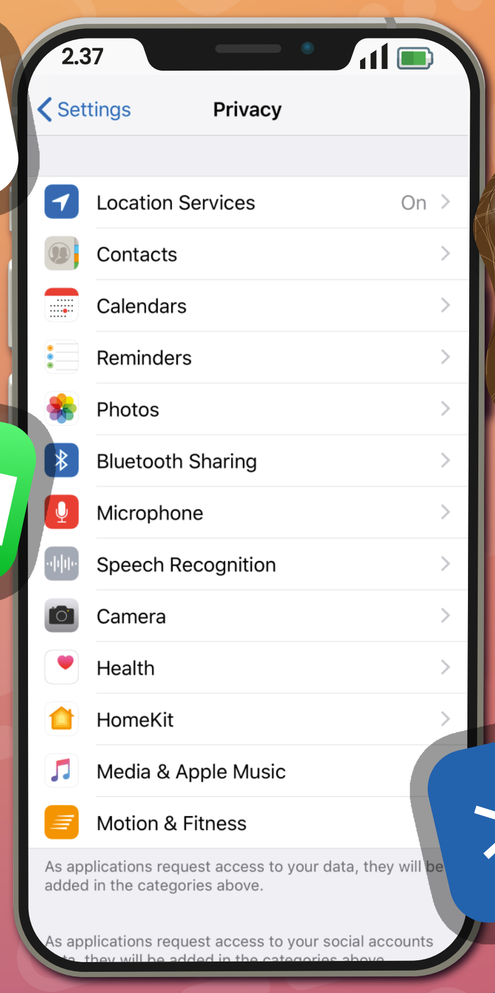
1. Open Google Play Family Link for parents
2. Tap the three horizontal lines in the top left
3. Select your child's account
4. Tap Manage
5. Tap Controls on Google Play
6. Tap Apps & Games
7. Select the age limit you wish to set

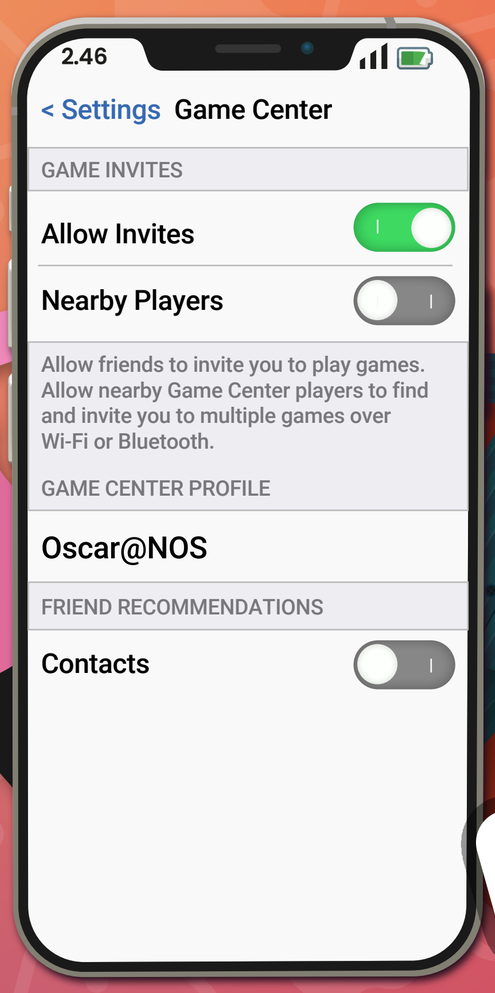
National Online Safety®
www.nationalonlinesafety.com

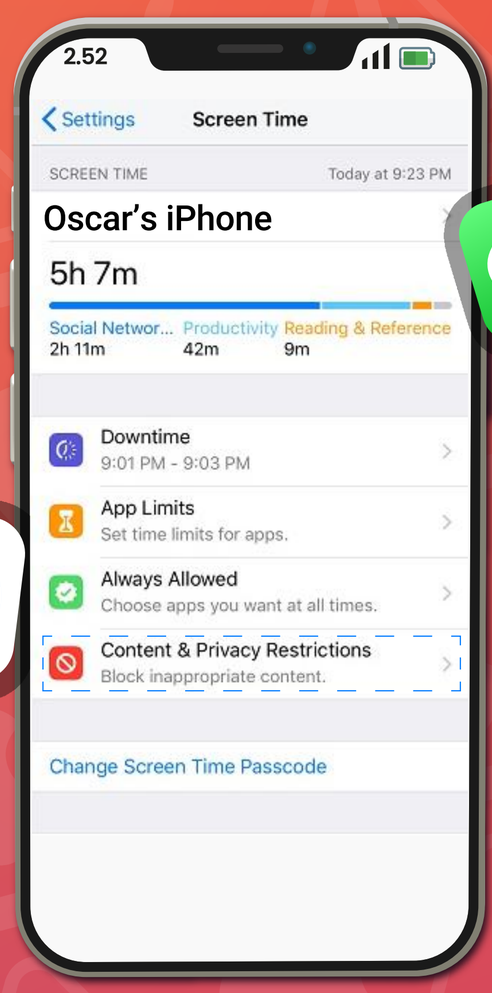
How to Set up PARENTAL CONTROLS for APPS

iPhone

Apple devices come with built-in apps already available: Mail, FaceTime and Safari, for example. However, you can choose which apps and features appear on your child's device and which ones don't. You can also manipulate the features in Game Centre to enhance your child's safety and privacy when playing games, as well as blocking iTunes or App Store purchases if you wish.







How to Restrict Built-in Apps/Features

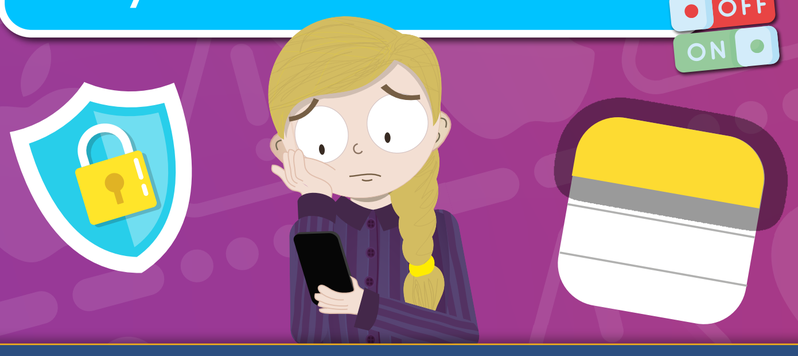
1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Allowed Apps (you may need to toggle this to 'on' at the top)
5. Enable or disable the apps you wish to appear(or disappear) on your child's device

How to Restrict Game Centre

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions (you may need to switch the toggle at the top to the 'on' position)
5. Scroll down to Game Centre
6. Choose between Allow, Don't Allow, or Allow with Friends Only in the settings for each feature

How to Restrict iTunes & App Store Purchases

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap iTunes & App Store Purchases
5. Select Allow or Don't Allow for each feature (you can also lock these settings with a password)



National Online Safety®
www.nationalonlinesafety.com

What Parents Need to Know about POKÉMON GO

AGE RESTRICTION PEGI 7

Pokémon GO has been among the world's most popular mobile games since its spectacular release in 2016. It's recently enjoyed a resurgence, thanks partly to people combining entertainment and exercise during lockdown. In Pokémon GO – like the Pokémon TV show, trading card series and other video games – players capture, train and battle with their Pokémon creatures: physically exploring locations while using augmented reality via their phone's screen. The game generally provides a positive experience, but there *are* still some safety concerns to consider.

ENVIRONMENTAL HAZARDS

Pokémon GO requires players to visit in-game landmarks like Pokéstops and Gyms. These are often situated at public real-world locations such as churches or post offices. Sometimes, however, they can inadvertently end up being placed in dangerous areas which are unsuitable for children, even when accompanied by an adult: near a construction site or a main road, for example.

STRANGERS & MEETING OFFLINE

Players often cooperate with friends in the game, and there are many online discussion hangouts. As well as sharing tips and info, these groups may arrange to meet offline to catch Pokémon or attend raids (communal events where players flock to the same real-world place for a mass battle). This can put children at risk of being messaged and invited to meet by strangers under the pretence of talking about the game.

DATA COLLECTION

When a player logs into their Pokémon GO account, the game collects personal data about the user and their device. Locations, emails, names, ages and even camera images can all be accessed. What then happens to this information is open to debate. Niantic, the game's developers, maintain that they do not sell user information to third parties – but the fact that they have it at all is a concern, nonetheless.

VISIBLE PROFILES & LOCATION

Pokémon GO players can add each other as 'friends' in the game by sharing their trainer codes. Two trainers who do this can then view each other's information, such as their username. If a username gives any clues to the player's real name or personal details, a stranger may then be able to look them up online. The game also lets users upload images to social media, which could publicly disclose a child's exact location.

IN-GAME PURCHASES

The game uses a currency called Pokécoins, which can be bought for real money (in bundles between £0.79 and £99.99) and exchanged for in-game items such as Pokéballs and berries. It's extremely easy for a child to purchase Pokécoins (even accidentally) if there's a payment method connected to their mobile phone – and possibly rack up a sizeable bill without realising it!

Advice for Parents & Carers

PLAY ALONGSIDE YOUR CHILD

Finding and catching Pokémon with young ones could turn into a great mutual hobby. At 25 years old, it's one of the few games franchises that spans two generations. Enjoying the game together will give you plenty of new things to talk about with your child – and if you played Pokémon in your own childhood, you might impress them with your knowledge of the digital critters!

ENCOURAGE AWARENESS

Remind your child of the physical dangers they could face while catching Pokémon and emphasise staying aware of their surroundings. The game will often alert children (through their phone) when they are close to an interesting Pokémon item – usually sending them excitedly rushing off to find it – so they should never play Pokémon GO near busy roads or in places they don't know well.

DISGUISE THE EXERCISE

One of Pokémon GO's benefits is that it encourages young (and not-so-young!) ones to get exercise outdoors. Some parts of the game can be completed from home, but it's best experienced while walking around your local area. Certain tasks (like visiting Pokéstops) can be repeated every day – and an hour outside having fun catching Pokémon will hardly feel like exercise at all!

USE AN OLDER PHONE

If children use an older phone to play Pokémon GO, then they won't be walking around with their own new device, which could get broken or stolen. Parents are also far less likely to have left a credit card linked to the old mobile. It also means that you can limit the amount of information used to set up an account, and what companies who gain access to your data can do with it.

AGREE PLAY BOUNDARIES

Ensure your child knows where they are (and aren't) allowed to go searching for Pokémon, when they have to be home, and how often they can play the game. Talk to other young Pokémon GO fans' parents or carers to see what boundaries they set for their children. Lunchtimes (if allowed by the school) or after school are ideal times for getting some exercise and catching all those Pokémon!

Meet Our Expert

Mark Foster has worked in the gaming industry for several years as a writer, editor and presenter. He is the gaming editor of two the biggest gaming news sites in the world: UNILAD Gaming and GAMINGbible. Having started gaming at a young age with his siblings, he has a passion for understanding how games and tech work – but, more importantly, how to make them safe and fun.

SOURCES: https://heimdalsecurity.com/blog/is-pokemon-go-safe/
https://bleedingcool.com/games/pokemon-go-announces-quality-of-life-updates-for-february-2021/

National Online Safety®
#WakeUpWednesday

What Parents and Carers Need to Know about ...

SOCIAL MEDIA SCAMS

On any social media platform, you'll often come across links to genuine-looking websites. They might include an exclusive offer for one of your favourite shops or invite you to complete a quiz in return for a particular reward. In some cases, clicking on these links takes you to a fake website where you are asked to provide your personal details. The whole enterprise is a ploy to capture sensitive details, such as your email address and password, which the scammers then exploit at your expense.

Clickjacking for fake rewards

Here, the attacker tries to lure you into clicking a link by offering something in return, such as a free gift for completing a survey. However, when the link is clicked, it collects the details of whoever fills out the survey. This might include full names, addresses, phone numbers and email addresses. Scammers could use these to hack into your other accounts or simply sell your data to other criminals.

Malicious app downloads

Some cybercriminals design software that appears genuine or helpful (and is normally free) but has been created to steal your personal information. There may be a pop-up ad encouraging you to download and install the app. Once the app is downloaded, the attacker can see any personal credentials you enter, and could then use this information for their own gain.

'Payment first' scams

Prevalent on sites such as Depop, these scams have spread to Facebook since it added the Marketplace feature. A user lists an item for sale and requests payment up front. Most online stores work this way, but the crucial difference is that scammers ask for payment via PayPal friends and family – *not* goods and services. This means you can't dispute the payment: the scammer keeps your money, and you never receive the item.

Threats disguised as quizzes

Most quizzes on social media seem harmless, but many come with hidden threats. When you submit your answers, you're also agreeing to terms and conditions which – in some cases – allow the quiz developer to sell your details to third parties. This puts you at greater risk of phishing attacks and spam advertising emails. It might also give the app permission to use information from your profile.

Untrustworthy URLs

It's common on social media for URLs in posts to be shortened (to meet Twitter's character count, for instance). This may seem harmless, but it opens an avenue of attack for scammers who may be disguising a malicious link as legitimate. These links can install malware on the victim's device, which could lead to passwords being stolen or even be the precursor to ransomware attacks.

Angler phishing scams

Using a fake corporate social media account, the scammer pretends to be from customer services. When someone complains about customer service on social media, the fake account messages them asking for their name, phone number and email. If the user provides this info, they are directed to a fake website where they enter their login details. The attacker can then steal their credentials or infect their device with malware.

Advice For Parents & Carers

Set strong passwords

Always ensure that your passwords are not easily guessable. Try to use a mix of letters, numbers and special characters so that criminals cannot forcefully get control. You should also change your passwords every so often to provide further protection against your accounts being taken over. If you have any concerns about your account's privacy, change the password.

Review your privacy settings

Regularly review your privacy settings on social media. You can restrict which parts of your profile can be seen and by who. We recommended making your personal information only visible to friends, which will help to limit the information a scammer could find out about you from social media. It's also safest to only accept friend or follow requests from people that you actually know.

Protect your personal information

Never enter personal information on unfamiliar websites. If you were redirected to a site from a social media post or an email link, putting in your personal details could give key information away to a scammer. Fraudsters may pose as someone you know to try and get your address or bank details (or your family's). If this happens, block the user and tell your family, so the scammer can't try to deceive anyone else.

Avoid opening suspicious emails

When you get an email, always check the sender's address before opening it. If it's an unexpected email and the sender is a stranger, mark it as junk (in case they try again in future) and simply delete it. They could be a scammer who's simply seen your email address on your social media profile. Being aware of phishing attacks is the primary method of defence against scam emails like this.

Choose trusted download sources

Don't download apps or files from unknown sites – instead, use verified and trustworthy sources (such as Google Play or the App Store for download to mobile devices). You can recognise safe sources by their trust seals. The browser address bar on a secure site starts "https" instead of "http". A shield or lock symbol in the address bar also indicates that a site is secure.

Install anti-virus software

Another key tip is to ensure that you have robust and reliable virus protection installed on any of your devices that support it. Anti-virus programmes will help to insulate you against cyber-attacks by blocking any malicious downloads or detecting any recently downloaded malware and removing it. Update your virus protection software regularly and carry out frequent scans of your device.

Meet Our Expert

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

KryptoKloud

NOS

National Online Safety®

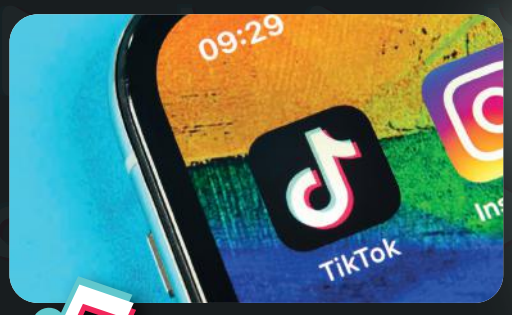
#WakeUpWednesday

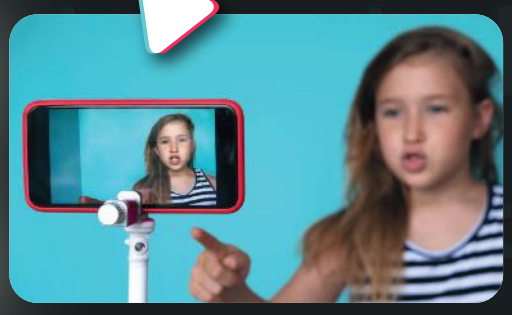
At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one app of many which we believe trusted adults should be aware of.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

TikTok is a video-sharing social media app which lets people create, view and download looping 15-second clips. Typically, these are videos of users lip-syncing and dancing to popular songs or soundbites (often for comic purposes), enhanced with filters, effects and text. Designed with young people in mind, TikTok skyrocketed in popularity in 2019 and has featured near the top of download charts ever since. It now has around 800 million active users worldwide.

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

What Parents & Carers Need to Know About TIKTOK





AGE-INAPPROPRIATE CONTENT

Most videos appearing on a child's feed are light-hearted and amusing. However, some clips have been reported for featuring drug and alcohol abuse, themes of suicide and self-harm, or young teens acting in a sexually suggestive way. The sheer volume of uploads is impossible to moderate entirely – so it *is* possible for a child to be exposed to explicit and age-inappropriate content.

EXPLICIT SONGS

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

TIKTOK FAME

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

HAZARDOUS VISIBILITY

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

ADDICTIVE NATURE

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

IN-APP PURCHASES

There's an in-app option to purchase 'TikTok coins', which are then converted into digital rewards for sending to content creators that a user likes. Prices range from 99p to an eye-watering £99 bundle. Buying coins is now restricted to over-18s – but TikTok doesn't require users to verify their age on sign up, so a young person could easily access this feature if they were determined to.

National Online Safety®
#WakeUpWednesday

Advice for Parents & Carers

TALK ABOUT ONLINE CONTENT

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

MAINTAIN PRIVACY SETTINGS

In early 2021, TikTok changed the default setting for all under 16s' accounts to 'private'. Keeping it that way is the safest solution: it means only users who your child approves can watch their videos. The 'Stitch' (which lets users splice clips from other people's videos into their own) and 'Duet' (where you build on another user's content by recording your own video alongside their original) features are now only available to over 16s. This might clash with your child's ambitions of social media stardom, but it will fortify their account against predators.

LEARN ABOUT REPORTING AND BLOCKING

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

ENABLE FAMILY SAFETY MODE

'Family Safety Mode' lets parents and carers link their own TikTok account to their child's. Through your mobile, you can control your child's safety settings remotely – including limiting screen time, managing their ability to exchange messages (and with whom) and blocking a lot of age-inappropriate content. Tiktok refreshed its Safety Cantre in May 2021, providing new resources for parents and carers to support online safety among families. These resources can be found on their website.

USE RESTRICTED MODE

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

MODERATE SCREEN TIME

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

Meet our expert

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

SOURCES: www.tiktok.com