A-PDF To Image DEMO. Purchase from www.A-PDF.com to remove the watermark

National Online Safety

7 questions to help you start a conversation with your child about online safety

#WakeUpWednesday

1 Which apps/games are you using at the moment?

THIS WILL GIVE YOU A GOOD OVERVIEW OF THE TYPES OF THINGS YOUR CHILDREN ARE DOING ON THEIR DEVICES, ALONG WITH THEIR INTERESTS. REMEMBER THAT THEY MIGHT NOT TELL YOU EVERYTHING THEY ARE USING, SO IT IS A GOOD IDEA TO ASK THEM TO SHOW YOU THEIR DEVICE. BECAUSE NEW APPS AND GAMES ARE RELEASED REGULARLY, IT IS IMPORTANT TO HAVE THIS CONVERSATION OFTEN TO ENSURE YOU ARE UP TO DATE WITH WHAT THEY ARE DOING.

2 Which websites do you enjoy using and why?

AS IN THE TIP ABOVE, ASKING THIS QUESTION WILL ALLOW YOU TO FIND OUT WHAT YOUR CHILD IS DOING ONLINE, AND ENCOURAGE POSITIVE CONVERSATIONS ABOUT THEIR ONLINE ACTIVITY. ASK THEM HOW THEY USE THE WEBSITES, AND TAKE AN INTEREST IN HOW THEY CAN USE THEM IN A POSITIVE WAY, ALSO ASKING THEM TO SHOW YOU IF POSSIBLE.

3 How does this game/app work? Can I play?

PLAY AGAIN? YES NO

SHOW A GENUINE INTEREST IN WHAT THEY ARE DOING. WHILST YOU ARE PLAYING A GAME OR USING AN APP WITH THEM, IT MIGHT HIGHLIGHT SOMETHING THAT THEY DON'T NECESSARILY THINK IS A DANGER TO THEM. IF THEY ACT LIKE THEY DON'T WANT TO SHARE THEIR ACTIVITIES WITH YOU, QUESTION WHY.

4 Do you have any online friends?

CHILDREN CAN FORM POSITIVE RELATIONSHIPS WITH PEOPLE ONLINE, AND THIS HAS BECOME MORE COMMON THANKS TO ONLINE MULTI-PLAYER OPTIONS, BUT THEY MAY NOT FULLY UNDERSTAND THE DIFFERENCE BETWEEN A FRIEND AND A STRANGER. YOU COULD MAKE THE QUESTION MORE SPECIFIC TO YOUR CHILD, FOR EXAMPLE: "HAVE YOU MET ANYONE ONLINE THAT YOU LIKE TO PLAY GAMES WITH?" THEY MAY NOT WANT TO SHARE THIS INFORMATION WITH YOU, SO ENSURE YOU TEACH THEM ABOUT HEALTHY RELATIONSHIPS.

5 Do you know where to go for help?

Childline 0800 1111

ALTHOUGH YOU MAY BE THE ADULT THEY TRUST THE MOST, SOME CHILDREN STRUGGLE TO TALK ABOUT WHAT HAPPENS ONLINE DUE TO CONFUSION OR EMBARRASSMENT. BECAUSE OF THIS THEY MAY STRUGGLE TO APPROACH THE NORMAL PEOPLE WHO WOULD HELP, SUCH AS YOURSELF OR A TEACHER. HAVE A CHAT TO YOUR CHILD ABOUT EXACTLY WHERE THEY CAN GO FOR HELP, AND HOW THEY CAN REPORT ANY ACTIVITY THAT THEY BELIEVE IS INAPPROPRIATE ONLINE.

6 Do you know what your personal information is?

YOUR CHILD MAY ALREADY KNOW WHAT THEIR PERSONAL INFORMATION IS BUT THEY MIGHT NOT THINK ABOUT HOW IT CAN BE SHARED. HAVE A CONVERSATION ABOUT WHAT PERSONAL INFORMATION IS AND HOW THIS CAN AFFECT THEM IF IT IS SHARED BEYOND THE INTENDED RECIPIENT. IT IS IMPORTANT THAT YOUR CHILD UNDERSTANDS THE DANGERS OF SHARING CONTACT DETAILS OR PHOTOS, AS INFORMATION SUCH AS THIS CAN SPREAD QUICKLY ONLINE.

7 Do you know your limits?

CHILDREN MAY NOT UNDERSTAND THE NEGATIVE IMPACTS OF DEVICE OR GAME ADDICTION. TALK TO THEM OPENLY ABOUT HEALTHY HABITS AND ASK WHETHER OR NOT THEM SPENDING TIME ONLINE OR PLAYING A GAME IS AFFECTING THEIR SLEEP, PERFORMANCE AT SCHOOL OR IF THEY ARE GENERALLY LOSING INTEREST IN OTHER ACTIVITIES. YOU MAY LEAD ON TO ENCOURAGING ALTERNATIVE ACTIVITIES AND DISCUSSING THE INTRODUCTION OF TIME LIMITS WHEN AT HOME.

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

Children are using smart devices from a much younger age than ever before. It's why it's essential we talk to our children about how to use them safely. There are so many positive benefits to the new technology at our disposal these days - however there are plenty of downsides too. As a parent, it's important you understand these risks and how you can take steps to protect your family against them.

1 PUT YOURSELF IN CONTROL

Make use of the parental control settings available to you. With most devices, you're able to change the settings to control the content your child has access to. This isn't difficult to do, as you'll often find guidance in the instructions that come with the device. By setting a private pin code on certain devices, you can make sure your child can only access it when you allow it.

2 PROTECTING ANDROID DEVICES

You can set up restricted users on Android tablets through a Google account. Open the settings menu (look for a cog icon) and select the 'Users' option. Here you can add a new restricted user. After setting up a password and username, select which applications you want to restrict access to. On an Android smartphone it's similar, but first select 'Parental Controls' in the play store.

3 PROTECTING APPLE DEVICES

For Apple devices, you can simply visit the preferences/settings menu and within 'General' there is an option for 'Restrictions'. Here you can turn off any applications or features on your child's device that you do not want them to have access to.

4 THINK ABOUT ALL YOUR SMART DEVICES

As well as tablets and smartphones, you should think about any device in your home connected to the Internet: a games console, a media hub, or a personal computer. In each case you can usually find parental controls in the settings. Think carefully about how much access you want to allow your child, especially when it comes to accessing the Internet.

5 MAKE SEARCHING MUCH SAFER

Most search engines, such as Google, Bing or Yahoo, have a 'safe search' setting. You should activate this. Otherwise, it's extremely easy for a seemingly harmless search on the Internet to return unexpected and inappropriate results. Depending on the browser you're using, go to the settings and search for 'safe search'. Make sure you save the change so it defaults each time you open the browser. This will seriously reduce the chances of your child being exposed to something they shouldn't be.

National Online Safety®
#WakeUpWednesday

9 Top Tips To Get Smart About children's devices

6 REGULARLY CHECK SOCIAL MEDIA SETTINGS

Before you allow your child to use social media, you should discuss the dangers with them. You should also make sure you're able to access their profile and privacy settings and check them regularly. The companies behind social media platforms often make privacy changes without making it very obvious to the user, such as Facebook's introduction of facial recognition software.

7 DON'T LET PEOPLE SEE WHERE YOU ARE

Location software sounds useful for seeing where your child is, but it also provides the opportunity for others to locate your child too. For safety, it's a good idea to disable location software on all devices or at least turn it off when it's not required. Also, be mindful of specific apps that record running routes or locations where your child might be playing a game. Talk to your child about why these can be dangerous and how to turn the setting on and off as required.

8 WATCH OUT FOR FAKE PROFILES

Sadly, social media presents an enormous opportunity for the likes of paedophiles to set up fake profiles and interact with children. Keep a track of the people your child interacts with on social media and if you do not recognise a user as a friend, consider blocking them.

9 KEEP A CHECK ON SCREEN TIME

Managing how much time we spend on screens is a new challenge for us all. It's critically important when it comes to children, especially younger children who are still developing. It's not just a case of setting arbitrary time limits. Guidelines published by The Royal College of Pediatrics and Child Health suggests it's more important to consider the 'context and content' of what the screen is being used for. Still, it is helpful to put limits on devices using 'Guided Access' functions, which you can find in the settings of certain devices.

Meet our expert

Emma Davis was a secondary school Computer Science teacher for more than decade. Since leaving education, she has been working in a cyber security firm delivering cyber awareness training to businesses and carrying out network testing. She is a mother of a five-year-old, she's had vast experience of controlling and managing how children access online services and use apps.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 10.04.2019

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

Publish date: 03.04.19

In today's digitally connected world, children and adults are constantly presented with new ways to engage, react and contribute. We're sociable beings; it's a natural human instinct, especially amongst younger audiences, to want to belong and join in. Viral Challenges (as they're often known) draw on these emotions and, as the name suggests, spread and gather pace very rapidly. New challenges are constantly emerging and evolving. They're often completely innocent, raising awareness of worthy causes or simply providing amusement. However, they can have much more sinister undertones, putting children at risk of physical harm or, in extreme cases, fatal injury.

What parents need to know about ONLINE CHALLENGES

MENTAL HEALTH & WELLBEING

As well as having the potential to cause actual physical harm, some challenges can be extremely upsetting for children. Many are created with the sole purpose of instilling fear in an individual in order to coerce them into doing things that could have a long-term emotional effect on them.

VARYING LEVELS OF RISK

As a parent or carer, it's important to take a balanced view and understand that not everything online has the potential to do harm. Mass-following and interaction can be a force for good. For example, the Ice Bucket Challenge, which swept the nation, set out to raise money and awareness of Amyotrophic Lateral Sclerosis (ALS). At its height, over 28 million people uploaded, commented on, or liked Ice Bucket Challenge related posts on Facebook. It's equally important to be aware though that online challenges often have a darker side. Malicious trends and challenges can expose children to dangerous or even life-threatening situations, so it's critical that parents and carers are aware of the latest risks and understand what steps to take to mitigate them.

'FOMO' - FEAR OF MISSING OUT

The 'Fear of Missing Out' (FOMO) is a strong emotional characteristic, particularly displayed in young people. The nature of viral challenges encourages children to explore and push boundaries. They tap into FOMO by feeding on a child's natural desire to join in, be accepted and share experiences with their friends and the wider online community. A recent study also found that FOMO is one of the greatest causes of Social Media addiction.

National Online Safety®

STRIVING FOR LIKES

In a major study by the Children's Commissioner, it was found that children as young as ten years old are reliant on 'Likes' for their sense of self-worth. A major concern around viral challenges is not knowing how far children will go to earn 'Likes'. Couple this growing appetite for acceptance with commonplace peer pressure and the potential problem is compounded. The result is that when young people are drawn into online challenges, because it is what all their friends are doing, saying 'no' can seem like a very hard thing to do.

"The coolest person at school will start a trend and then everyone copies her"
Merran, 12, Year 7

"If I got 150 likes, I'd be like that's pretty cool it means they like you"
Aaron, 11, Year 7

Top Tips for Parents

COMMUNICATION & MONITORING

It's important to talk to your child regularly and monitor their online activities. Encouraging honesty and openness, will give you a much clearer viewpoint of how your child is interacting online and what concerns they have. Create an atmosphere of trust. Ensure they feel they can confide in you or another trusted adult regarding anything they may have seen or experienced online that's upset them.

THINK BEFORE ACTING

As with most concerns in life, let common sense prevail when it comes to Viral Challenges. Young people need the freedom and space to explore and going in all guns blazing may well be counter-effective. Address the importance of safety and wellbeing, both online and offline, by getting the facts and understanding the risks. Start a discussion about the Online Challenges that may have captured your child's interest, gauge their likely involvement and explain the importance of thinking and acting independently when it comes to participating.

SETTING UP EFFECTIVE PARENTAL CONTROLS

As with all online activity, ensuring you have effective parental controls set up on all devices will help filter and restrict the dangerous or inappropriate content you don't wish your child to access. Additional measures for protecting your child include checking the privacy settings on your child's devices, monitoring their friends list, ensuring their personal information is safe and secure and keeping a watchful eye on the content they're sharing.

REPORTING & BLOCKING

Parental controls can only go so far in blocking potentially harmful content. A rise in the decoding of social media algorithms, has led to age inappropriate content increasingly appearing on platforms and apps used by children. Where possible, you should regularly monitor what your child sees online and flag/report any content which is inappropriate or dangerous. You should take the time to talk to your child, define what you consider to be appropriate content and show them how to report and block users/accounts themselves.

VALIDATE SOURCES

Not everything is as it seems. Some people create fake content that's designed to 'shock' in order to encourage rapid sharing. If your child has seen something online that has triggered concern you should encourage them to, check its origin, verify that it came from a credible source and check the comments made for any clues to its validity.

FACING REALITY

Trends and Viral Challenges can be tempting for children to take part in; no matter how dangerous or scary they may seem. As a parent or carer it can be difficult to keep pace with the very latest Online Challenges emerging. In recent months these have included potentially dangerous crazes, including the 'Bird Box' challenge, which was inspired by Netflix's popular film and encourages followers to upload videos of themselves attempting everyday tasks while blindfolded. The best advice is to keep talking to your child. Show that your taking an interest and not just prying. Ensure your child knows they don't have to get involved and if they're unsure, let them know you're there to talk before they consider participating. Children often need reassurance that not everything they see online is real. If your child has viewed distressing or frightening content it's important to talk to them about their experience, support them and, if required, help them find additional support.

SOURCES:
https://www.independent.co.uk/news/science/fake-news-twitter-spreads-further-faster-real-stories-retweets-political-a8247491.html | https://www.dailymail.co.uk/news/article-2209452/Teen-dies-copying-pass-game-time-YouTube.html
https://www.dailymail.co.uk/news/article-6307331/Boy-11-dies-YouTube-choking-challenge-mother-warns-parents-son-strangled-himself.html | Children's Commissioner Life in 'likes' report - RSPH - Status of mind report
https://www.bbc.co.uk/news/magazine-29013707 | https://www.independent.ie/life/health-wellbeing/fear-of-missing-out-fomo-one-of-greatest-causes-of-social-media-addiction-study-finds-36975296.html
http://www.ttlp.co.uk/news/children-as-young-as-eight-addicted-to-social-media-likes/

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 03.04.19

What children need to know about

ONLINE BULLYING

What is online bullying?

ONLINE BULLYING – ALSO KNOWN AS CYBERBULLYING – IS BULLYING THAT TAKES PLACE ON THE INTERNET OR VIA ELECTRONIC DEVICES AND MOBILE PHONES. IT CAN INCLUDE:

1. SENDING SOMEONE MEAN OR THREATENING EMAILS, DIRECT MESSAGES OR TEXT MESSAGES
2. HACKING INTO SOMEONE'S ONLINE ACCOUNT
3. BEING RUDE OR MEAN TO SOMEONE WHEN PLAYING ONLINE GAMES
4. POSTING PRIVATE OR EMBARRASSING PHOTOS ONLINE OR SENDING THEM TO OTHERS
5. CREATING FAKE SOCIAL MEDIA ACCOUNTS THAT MOCK SOMEONE OR TRICK THEM
6. EXCLUDING SOMEONE FROM AN ONLINE CONVERSATION OR BLOCKING THEM FOR NO REASON

BE KIND ONLINE

BEFORE PRESSING 'SEND' ON COMMENTS, ASK YOURSELF THESE 3 QUESTIONS...

1. WHY AM I POSTING THIS?
2. WOULD I SAY THIS IN REAL LIFE?
3. HOW WOULD I FEEL IF SOMEBODY SAID THIS TO ME?

National Online Safety

#WakeUpWednesday

Why does it happen?

GOING ONLINE MAKES IT EASIER FOR PEOPLE TO SAY AND DO THINGS THEY PROBABLY WOULDN'T DO FACE TO FACE. ONLINE BULLIES DON'T GET TO SEE THEIR VICTIMS' REACTIONS IN REAL LIFE, SO THIS CAN COCOON THEM FROM THE REAL DAMAGE THAT THEY ARE DOING. QUITE OFTEN, PEOPLE BULLY BECAUSE THEY ARE GOING THROUGH SOMETHING DIFFICULT THEMSELVES AND TAKING IT OUT ON OTHERS IS THE ONLY WAY THEY KNOW HOW TO GET CONTROL OF THEIR OWN EMOTIONS.

How does it feel to be bullied?

BEING BULLIED CAN IMPACT ON YOUR SELF-ESTEEM, CONFIDENCE AND SOCIAL SKILLS. BECAUSE IT HAPPENS ON YOUR PHONE, TABLET OR COMPUTER, IT CAN FEEL LIKE YOU ARE UNDER THREAT EVEN WHEN YOU'RE IN A SAFE ENVIRONMENT, SUCH AS YOUR BEDROOM. DON'T FORGET...IT IS NOT YOUR FAULT IF YOU'RE BEING BULLIED.

Am I an online bully?

SOMETIMES IT ISN'T OBVIOUS THAT WHAT YOU ARE DOING IS WRONG, BUT IF YOU USE DIGITAL TECHNOLOGY TO UPSET, ANGER OR EMBARRASS SOMEONE ON PURPOSE, THIS MEANS YOU'RE INVOLVED IN ONLINE BULLYING. IT MIGHT BE AS SIMPLE AS 'LIKING' A MEAN POST, LAUGHING AT AN ONLINE VIDEO, OR SPREADING A RUMOUR, BUT THE PERSON BEING BULLIED COULD FEEL LIKE THEY ARE BEING GANGED UP ON. THINK ABOUT HOW IT WOULD MAKE YOU FEEL IF IT HAPPENED TO YOU. EVERYONE CAN MAKE MISTAKES, BUT IT'S IMPORTANT TO LEARN FROM THEM – GO BACK AND DELETE ANY UPSETTING OR NASTY POSTS, TWEETS OR COMMENTS YOU'VE WRITTEN.

Who do I tell?

YOU DON'T HAVE TO DEAL WITH THE BULLYING ON YOUR OWN. TALK TO AN ADULT THAT YOU TRUST – A PARENT, GUARDIAN, OR TEACHER. MOST WEBSITES, SOCIAL MEDIA WEBSITES AND ONLINE GAMES OR MOBILE APPS LET YOU REPORT AND BLOCK PEOPLE WHO ARE BOTHERING YOU. YOU COULD ALSO CONTACT CHILDLINE (WWW.CHILDLINE.ORG.UK), WHERE A TRAINED COUNSELLOR WILL LISTEN TO ANYTHING THAT'S WORRYING YOU – YOU DON'T EVEN HAVE TO GIVE YOUR NAME.

How do I prove it?

WHEN CYBERBULLYING HAPPENS, IT IS IMPORTANT TO DOCUMENT AND REPORT THE BEHAVIOUR, SO IT CAN BE ADDRESSED – RECORD THE DATES AND TIMES WHEN CYBERBULLYING HAS OCCURRED, AND SAVE AND PRINT SCREENSHOTS, EMAILS, AND TEXT MESSAGES.

How can I stay safe?

MAKE SURE YOUR PRIVACY SETTINGS ARE SET SO THAT ONLY PEOPLE YOU KNOW AND TRUST CAN SEE WHAT YOU POST. NEVER GIVE OUT PERSONAL INFORMATION ONLINE, SUCH AS IN PUBLIC PROFILES, CHAT ROOMS OR BLOGS, AND AVOID FURTHER COMMUNICATION WITH THOSE SENDING THE MESSAGES. KEEP AWARE OF FAKE PROFILES AND INTERNET USERS PRETENDING TO BE SOMEONE THAT THEY ARE NOT.

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 issue 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 AGE-INAPPROPRIATE CONTENT

"Inappropriate" means different things to different people. What's acceptable for one age group, for example, may be unsuitable for a slightly younger audience. Online, young people can chance upon inappropriate content in various ways – from pop-up ads to TikTok videos. The increasingly young age at which children become active in the digital world heightens the risk of them innocently running into something that they find upsetting or frightening. Trusted adults need to be able to help children be aware of what to do if they're exposed to age-inappropriate content.

WHERE IS IT FOUND?

SOCIAL MEDIA

Age-inappropriate content is easily accessible through many social media platforms. TikTok, for instance, is hugely popular with young people but is arguably best known for clips featuring sexualised dancing or profanity. Some social media users also express hate speech or promote eating disorders and self-harm, which could cause lasting damage to a child's emotional and mental health.

GAMING

Gaming is an enjoyable source of entertainment, but many popular titles can expose children to inappropriate material such as violence, horror, gambling or sexually explicit content. Playing games unsuitable for their age risks normalising to children what they are seeing. Some games also include in-game chat, where other (usually older) online players often use language that you probably wouldn't want your child to hear or repeat.

STREAMING

The range of video streaming services available online means that users can find almost anything they want to watch on demand. Children are therefore at risk of viewing TV shows and movies which contain nudity, drug and alcohol abuse, explicit language and extreme violence. Unfortunately, these streaming platforms can't always determine that it's not an adult who's watching.

ADVERTS

Online adverts frequently include age-inappropriate content: usually gambling and nudity or partial nudity, although adverts for alcohol or e-cigarettes are also common. Some search engines also feature adverts that are responsive to your search history: so if you've recently looked up a new horror movie, shopped for lingerie or ordered alcohol online, then the ads appearing on screen could reflect this the next time your child borrows your device.

18 Advice for Parents & Carers

TALK IT THROUGH

Embarrassment or fear of getting into trouble can make it difficult for children to talk openly about age-inappropriate content they've watched. Remind your child they can always come to you if they're troubled by something they've seen online, without worrying about consequences. Before offering advice, discuss what they saw, how they felt and how they came to find the content in question.

CONNECT, DON'T CORRECT

If your child's been particularly distressed by exposure to content that wasn't suitable for their age, it's important to offer guidance to prevent them from repeating the same mistake – but it's equally vital to help them deal with the emotions that the situation has raised. You could tell them about any similar experiences you might have had at their age, and how you dealt with it.

BLOCK, REPORT, CONTROL

After discussing the problem, you and your child can take action together. This could include blocking any inappropriate sites and reporting any content which violates a platform's rules. To further safeguard your child online, set up parental controls on internet-enabled devices that they use. This will significantly reduce the chances of your child being exposed to age-inappropriate content in future.

GET SPECIALIST HELP

Age-inappropriate content can potentially have a negative impact on a child's mental health, which is sometimes displayed through changes in their behaviour. If the problem becomes more severe, you might consider reaching out to a mental health professional or an expert in this field who can provide you and your child with the proper support.

STAY CALM

Even though it is obviously difficult to stay rational in a situation where your child has been put at risk, it's essential to think before you react. Your child may well have hesitated to open up to you about watching inappropriate content for fear of the consequences, so being calm and supportive will reinforce the notion that it would be easy to talk to you about similar issues in the future.

Meet Our Expert

Cayley Jorgensen is a Registered Counsellor with The Health Professions Council of South Africa, and she runs a private practice offering counselling to children, teenagers and families. Her main focus is creating awareness and educating the community on the mental health pressures of today's world, as well as resources and techniques to understand and cope better.

National Online Safety®

#WakeUpWednesday

Sources: https://www.educationvic.gov.au/documents/about/programs/bullyingoneans/inappropriate.pdf | https://www.esafety.gov.au/educators/training-professionals/professional-learning-program-teachers/inappropriate-content-factsheet | https://www.swalingreality.co.uk/wp-content/uploads/2021/04/childrens-media-lives-year-7.pdf

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.12.2021

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 of many apps 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 THE METAVERSE

AGE RATING: Varies per metaverse platform

'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.

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.

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.

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.

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.

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 Fornite, Minecraft, Roblox, Apex Legends and Valorant for HarperCollins and Bonnier Books.

GM W3

NOS National Online Safety®

#WakeUpWednesday

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

'Apps' are designed to run on certain devices and are written for a specific operating system, such as Apple iOS, Windows, or Android. The official store for the Apple iOS operating system is known as the 'App Store' and it's where you can browse and download more than 2 million apps and games to use on the iPad, iPhone, iPod Touch and other Apple devices. When your children are using the app store, you need to be aware of the risks...

What parents need to know about The App Store

IS YOUR CHILD 13+?

To download and buy apps from the App Store, your child will need an Apple ID. If they have used other Apple services, such as iCloud, they can sign into the App Store with the same Apple ID. If they are aged 13 and under, they cannot sign up for an Apple ID on their own, but an adult can create an Apple ID for a child.

IN-APP PURCHASES

Apps are either free, paid for or free with in-app purchases. In-app purchases are optional transactions that can unlock extra functionality, virtual goods or unique content. Unless you change the settings, once your child has entered a password to make an in-app purchase, they can make additional purchases for 15 minutes without re-entering a password. This makes it extremely easy for children to accidentally run up huge bills.

LOOKALIKE APPS

Some developers release apps that copy the functionality, user interface and even product names and branding of popular apps, in an attempt to trick unsuspecting users to install them. By downloading an app from an unknown developer, your child could find their device compromised. Experts warn that through app permissions, hackers can potentially take photos using the camera and access media remotely, track your child's location, record any passwords they enter for other accounts, and send text messages from phones.

INAPPROPRIATE APPS

Some apps and games have content that is unsuitable for younger children – even the most popular or innocuous looking apps may feature adult themed content, violence or cruelty to other people or animals, unmoderated chat, pornographic or sexual content.

THIRD-PARTY APP STORES

Because the official Apple App Store has a very stringent policy about what apps it approves, children may look elsewhere for apps and games they've heard about from friends. As well as the Apple App Store for iOS, there are hundreds of other third-party app stores, but the danger is they may not apply the same level of scrutiny toward the apps they allow to be listed. There's a higher chance of apps that infect devices with malicious codes or put user privacy at risk by extracting sensitive information.

Top Tips for Parents

CREATE YOUR CHILD'S ACCOUNT

You can create an Apple ID for a child under 13 and add them to your family group to keep an eye on their activity. Go to Settings > [your name] > Family Sharing > Add Family Member > Create a Child Account > Next. Enter your child's birthday and tap Next. Review the Parent Privacy Disclosure and tap Agree. With Family Sharing, you can add up to six family members to share App Store purchases, as well as iTunes and Apple Books.

SWITCH ON 'ASK TO BUY'

If you have a child that is over 13 years of age and has their own Apple account, make sure that you only allow them to make purchases with gift cards. You can also activate the 'Ask to Buy' feature if you are using Family Sharing, so that whenever a family member who isn't an adult initiates a new purchase, a request goes to the account organiser. You can also limit what content your child can access on the devices they use.

RESTRICT IN-APP PURCHASES

You can restrict your child's ability to make in-app purchases. On an iOS device, open Settings, tap General and then Restrictions. Tap 'Enable Restrictions'. You can put a limitation that requires a password every time there is a purchase made in the App Store or iTunes Store.

BROWSE APPS BY AGE

To find apps and games that are right for your children, check the age ratings. On an iPhone or iPod Touch, this can be found in the information section on an app's product page, and on an iPad or desktop, the age range is near the Buy button. On the Kids page, you can find apps for age ranges, including 5 and under, 6 to 8, and 9 to 11.

AVOID OTHER APP STORES

Put a rule in place that your child can only use the official App Store to download apps and games. Explain why it is wise to only install applications from a trusted source to ensure their device is not affected by security issues or virus attacks.

HOW TO KNOW AN APP IS SAFE TO INSTALL

Advise your child that just because they're downloading an app from an official store, it doesn't make it safe. Fake or copycat apps will often include misspelt words and poor grammar, so always read the app description, and double check the developer name and title for warning signs. Be wary of apps that come with a long list of permission requests. Check the app's reviews and ratings – one star, one line reviews complaining that an app didn't work on a certain device, or that there was a billing issue, is not a good indication.

SPOT FAKE REVIEWS

When checking the customer reviews within the app store, make sure they aren't vague and generic, or overly effusive, as some developers will try to manipulate their apps' positions by posting fake ratings and reviews. Check the number of downloads the app claims to have – the higher the number, the more likely it is to be safe. Your child can also check on a company's website to see if the app is available on there.

National Online Safety

A whole school community approach to online safety

www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061

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

PARENTING GAMERS

Moving from policing to parenting your gaming kids: how to engage and guide

With concerns about escalating screen-time, the impact of violence, unexpected costs and interloping strangers it can be tempting to lock down video games to limit their negative impact. While some sensible boundaries are helpful, they are only a short term solution for how we guide children towards gaming health. Like other areas of childhood, parents and carers can have a powerful steering presence by engaging and participating in the video games their children play. This not only reduces risks because they are aware of the kinds of activities, interactions and costs involved but makes video games a part of family life. Along with building dens, climbing trees, cooking and family walks, playing games with children enables parents to guide the quality of content being played. This may start with sharing the games children are currently playing, understanding why they love it and celebrating successes. But with a little research, this can grow into suggesting other games to play and higher ambitions for what kids get out of playing long-standing favourites.

National Online Safety®

A New Media For Everyone

Video games are a new kind of media. Because they are new we don't entirely understand their potential yet. They've become hugely popular and commercially successful as blockbuster entertainment for children and teenagers. However, like books, films and music, the real range of video games on offer is much broader than this.

There are games about every topic you could imagine, and aimed at a wide range of ages and perspectives. Whether it's sharing a families heartbreaking story in That Dragon, Cancer, stepping into the shoes of a Syrian migrant in Bury Me, My Love, or taking the hand of your child and soaring over the clouds in Sky: Children of Light, games take us places in unique ways. It's no surprise, then, that Newzoo figures show that in 2018 40% of men and 32% of women play games. And Entertainment Software Association (ESA) data showed that the average age for US gamers is 34 for women and 32 for men.

If you want to turbocharge your care of a child who loves playing video games, the best thing to do is to find games you want to play yourself. This can sound like strange advice until we consider how hard it would be caring for a child who loves books without reading ourselves or guiding a child who loves music without sharing our favourite songs.

Video Game Diet

Gaining an understanding of what video games are, what they are like to play and the different experiences on offer, enables you to encourage a varied gaming diet. Similar to how we don't worry about plate-time but what's on the plate, we can differentiate between different types of screen experience.

Playing Fortnite offers exuberant excitement and connection to friends. Playing Mario Kart connects us to the players sitting next to us. Roblox can be a place for children to play at having a job or surviving a storm. Minecraft can be a tranquil escape from a busy day at school. Alto's Adventure can be a way to calm anxiety or jangling nerves.

Parents and carers can expand these experiences. Kingdoms Two Crowns, Reigns and Life is Strange teach players to trust their instincts in game-worlds built to encourage risk and hunch taking. Florence, Abzu, Journey and Brothers Tale of Two Sons are a gentle way for children to learn about their own emotional responses to challenging situations as well as appreciating how people experiencing them first hand may feel. Eco and One Hour, One Life encourage the altruism of building something that other players benefit from.

Creators Not Consumers

Ambition for their future means parents and carers support activities where children are excelling. While this is familiar territory when a child is brilliant at an instrument or learning a foreign language, it's easy to miss the need for our enthusiasm when it comes to video games. Along with the general connection and good feelings that come from a parent or carer celebrating success in an activity that a child enjoys comes the imperative that they could go further than they realise themselves. The rise in competitive video games can sound peculiar but requires great skill, draws large audiences and comes with high prize money for professional players. Beyond this, parents can guide children towards other careers in video games which need diverse creative, technical and social skills. A simple and effective way to do this is to encourage children to create as well as consume games. This can start as simple customisation of the games that allow you to design maps and characters. Then there are games like Mario Maker on Wii U, 3DS and Switch where you can design and share levels for other players. Dreams on the PlayStation 4 takes this further with an accessible game creator that's also really powerful.

Finding Games You Want Children To Play

Parenting rather than policing video games equips children to build good habits and a healthy relationship with digital media for when they leave home and parents aren't around to enforce the rules. One challenge can be finding the kinds of games you want your children to play. There are good resources to help you with this. Many of the examples here come from my upcoming Taming Gaming book: https://unbound.com/books/taming-gaming/
There are also websites that provide video game suggestions like AskAboutGames https://www.askaboutgames.com. Also, there are good Twitter accounts that help, like Wholesome Games (@_wholesomegames) and Non-Violent Game Of The Day (@NVGOTD).

You can also use the VSC Rating Board (https://videostandards.org.uk/RatingBoard/) website and PEGI app to search for games of different ratings.

Meet our expert

Andy Robertson is a parent of three children and journalist who writes for national newspapers and broadcast television. His Taming Gaming book helps parents guide children to healthy play.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 31.07.2019

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

National Online Safety®

#WakeUpWednesday

Conversation starters for parents and carers: ONLINE CONTENT

Trying to start a conversation about online safety with children can be a daunting task. There are many reasons why children may not want to talk to adults about it. One might be that they don't think you'll understand or that you won't know how to help if they came to you with an online problem. It can also be hard to start a conversation about something that you might have limited knowledge about. However, with screen time increasing during the lockdown, it's important now more than ever, to be talking to children about what they are accessing online.

1 ASK THEIR MOTIVATION

Sometimes it's easy to assume we know why children choose certain games or apps. It can seem obvious, like the child interested in football will be enthusiastic about the new FIFA game. But sometimes it can be more subtle than that. It could be that it's an outlet for their creativity or it might be that they like the look of the main character. Learning their motivation and knowing why they like it can help advising them on how to use it safely and help you discuss the pros and cons.

2 CULTIVATE A BLAME FREE CULTURE

Children can often blame themselves if they come across something that scares them or makes them feel uncomfortable. There will be times when your child has gone against something that you have forbidden, however, most children do not intend to put themselves at risk. Therefore, it's important that your child is able to come to you with a problem and won't be blamed for it. Try to understand what happened and why and warn them of the dangers once more. Engaging in a 'told you so' dialogue or suggesting they are in trouble for not listening may deter them from reporting any future concerns.

3 SHARE PERSONAL EXPERIENCE

Starting a conversation by sharing something that you've seen or that has made you feel uncomfortable can be a great opener. Talking about your own feelings can help children realise that it isn't just them – adults can be affected too. You can then go into how you coped with it therefore indirectly giving children advice on how they can also cope in uncomfortable situations. You can also explain that the reason that you've chosen to talk to them about it is because talking helps. Children will hopefully be able to see the parallels in the experiences and mimic your behaviour in future.

4 TALK ABOUT THE NEWS

Asking children what their response is to news stories around online safety can be revealing. For example, there has been a recent survey conducted by the BBFC who are currently campaigning for the application of age ratings and content warnings on video sharing platforms. What do they think about this? Can they think of a time when this would have helped themselves or someone they know? Are they against the idea? If so, why? Could they be accessing something they shouldn't be?

5 ASK FOR ADVICE

It could be that you really do have a friend at work who is debating whether or not to let their child do something online, or it could be that you're bending the truth slightly, but hopefully the outcome would be the same. Don't be afraid to ask others for advice. Not only why they should let the child use it, but also what would they tell the child to be aware of. What are the risks? This will help you understand the risks yourself and what to look out for in future.

6 MAKE TIME TO LISTEN

When your child can't wait to tell you about their new game, always try and listen to what they say. We always have a lot on our minds, so it's easy for us to drift off onto other things which may be more important. However try to stay involved and ask them more details about aspects of the game/app. Children will appreciate your interest and the more questions you ask, the more you can find out. If you act uninterested, then they are less like to tell you about it again in the future.

7 ASK THEM TO BE THE TEACHER

Showing an interest in what children are accessing online is a great opportunity for you to learn something new as well. Children on the whole love sharing their experiences so by asking them to teach you how to use an app or play a game is not only a great way to bond, but you will also feel more empowered to talk about it. It is easy to shy away from conversations when the child perhaps knows more about the subject content than you do. This can help to turn this around.

8 USE SCHOOL MESSAGING

It might be that your child's school has sent out a message about the Childline number or to remind children to use the CEOP button to report content. Ask the children what they learned about these at school. When would they use the Childline number? When would they need to use the CEOP button? What does it look like? Asking the children why the school thought that the information was so important that they sent out a message about it reinforces what they learnt whilst at school.

9 ASK ABOUT THE RISKS

Many children may know what online risks are and will happily explain the potential dangers. Listen and try not to be overly shocked if they tell you something that disturbs you. This can then lead nicely into you asking the question about what steps they are taking to look after themselves or what help they could seek if something goes wrong. Sometimes it's just nice to know that your children know the dangers and have taken steps to help reduce the risk for themselves – this is the ultimate goal.

10 ASK ABOUT RESPONSIBILITIES

Try asking open ended questions about roles and responsibilities online. Who is in control of the internet? Who is looking after you whilst you are online? Who decides what is appropriate for children to see? This can reveal a lot about a child's perception about who is responsible for their online safety. If they believe that it is up to everyone else to keep them safe, then you know you need to have a conversation about how they can reduce their own risk.

11 ASK ABOUT SCHOOL ADVICE

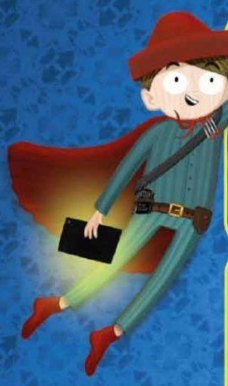
Sometimes it's hard to know what to warn children about. If there is a new app or game that your child has come across recently, ask them what they think their teacher would say about it. What advice would school give them? What have they been told about trusting people online or about fake news? Finding this out would be a good way to hear what advice they were given at school and help you reiterate the same message. Quick reminders about what to do if something makes them feel uncomfortable or who their trusted adults are can make all the difference.

Meet our expert

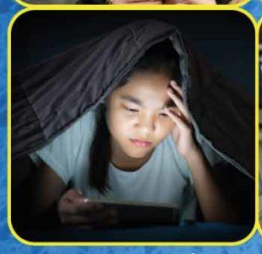
Heather Cardwell is a practising Online Safety Lead and senior school leader who is passionate about safeguarding children online and educating them around online risks. She has over 10+ years as a Computing Lead and has successfully developed and implemented a whole school approach to online safety in schools, delivering online safety training to both school staff and parents and helping to roll-out a bespoke online safety policy across her local network of education settings.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 24.06.2020



Grooming is when someone befriends and builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. They can do this both offline and online, with technology and the Internet being commonly used to initiate and facilitate contact with a child. Gaining victims' trust is a key part of engaging them in sexually explicit behaviour. The groomer, who can either be a stranger or someone a child already knows, tends to use tactics such as engaging in small talk or exchanging personal information with the child about hobbies and relationships, using flattery and gifts to build a rapport or even making threats and intimidation to gain control. This can take place over varying periods of time – from a few days to several years.



What parents need to know about ONLINE GROOMING

NUMBERS OF GROOMING OFFENCES ARE SOARING

In April 2017, a new government law came into force in England and Wales to allow police to charge adults who send sexual messages to children through mobile phones and social media. In the first year since the law change, there were 3,000 police-recorded offences of sexual communication with a child – a figure 50 per cent higher than experts expected in the first year.

ALL CHILDREN ARE AT RISK

According to a 2018 NSPCC report, a quarter of young people have experienced an adult who they don't know in real life trying to contact them online. One in four said they had been sent messages, images, videos or other content that made them feel sad, worried or uncomfortable. One in 10 girls and one in 20 boys under the age of 13 said they had received unwanted sexual messages.

CHILDREN ARE VULNERABLE TARGETS

Groomers use psychological tricks and methods to try and isolate children from their families and friends and will often choose to target more vulnerable children who may be easier to manipulate. In order to seek potential victims, predators are likely to use apps and websites that are popular with children and young people. Groomers can use a 'scattergun' approach to find victims, contacting hundreds online to increase their chance of success.

LIVE STREAMING CONCERNS

Predators may use live video to target children in real-time using tricks, dares or built-in gifts to manipulate them. Grooming often takes the form of a game where children receive 'likes' or even money for performing sexual acts. Social media channels, such as YouTube, Facebook, Instagram and Snapchat, all have live streaming capabilities, but there are many apps which children can use to live stream, including Omegle, Live.me, BIGO Live, YouNow and many more.

GROOMING CAN HAPPEN RAPIDLY

Grooming is generally a slow, methodical and intentional process of manipulating a person to a point where they can be victimised. However, according to researchers at the University of Swansea, online grooming can also be very rapid, with analysis of chat logs revealing that it can take just 18 minutes for some predators to arrange to meet their victim. The fastest predators used sophisticated, persuasive, language-based strategies to rapidly build trust, including the use of small talk and praise which quickly escalated into requests for sexual messages.

ANYONE CAN GROOM YOUR CHILD

Many people expect groomers to be adults posing as children, but this is not always the case. Data from University of Swansea reveals that groomers' use of identity deception (around age, location and appearance) is fairly low. This can be because they approach many children, limiting their ability to lie. The worry is that honesty can be more damaging to the victim since they are more likely to feel as if they are in a real relationship.

National Online Safety

Top Tips for Parents

IT'S GOOD TO TALK

It's unlikely that you can stop your child using the Internet, nor can you constantly monitor their online activities, but you can talk to your child on a regular basis about what they do online. By talking openly with them about online relationships, they can quickly ascertain the kind of behaviour which is appropriate or inappropriate. Ask them whether they have any online friends or if they play online games with people they haven't met. This could then open up conversations about the subject of grooming.

CHECK PRIVACY SETTINGS

In order to give your child a safer online gaming experience, it is important to check privacy settings or parental controls on the networks, devices, apps, and websites they may use. If you use location-sharing apps to check where your child is, remember that these could always be used by strangers to follow your child without their knowledge. Ensure that you check options so that location information is never shared with anyone except those they have permission to share with.

DISCUSS SAFE ONLINE BEHAVIOUR

Make it clear to your child that they should not accept friend requests from people they don't know and to verify friend requests with people who they do know. They should never agree to chat privately with a stranger or someone they don't really know. Remind them that they should never divulge personal information, such as mobile phone numbers, addresses, passwords or name of their school.

DISCUSS HEALTHY RELATIONSHIPS

Talk to your child about what a healthy relationship looks like and how to detect someone who might not be who they claim to be. Explain that groomers will pay your child compliments and engage in conversations about personal information, such as hobbies and relationships. They may admire how well they play an online game or how they look in a photo. Groomers will also try and isolate a child from people close to them, such as parents and friends, in order to make their relationship feel special and unique.

BE SUPPORTIVE

Show your child that you will support them and make sure they understand they can come to you with any concerns they may have. They need to know they can talk to you if someone does something they are uncomfortable with, whether that is inappropriate comments, images, requests or sexual comments.

LOOK OUT FOR WARNING SIGNS

Child safety experts have identified key grooming patterns and advise parents to look out for:

- Secretive behaviour about what they are doing online.
- Internet or smartphone usage late at night.
- Going to unusual places to meet up with friends you have not heard of.
- They are clingy, have problems sleeping and eating or even bedwetting.
- A lack of interest in extra-curricular activities.
- Having new items, such as clothes or phones, which they can't explain.
- They seem withdrawn, anxious, depressed or aggressive.
- Having older boyfriends or girlfriends.

HOW TO REPORT

If you're worried that your child is being groomed online or sexually exploited, you can report your concerns to the Child Exploitation and Online Protection (CEOP) Safety Centre, which is part of the National Crime Agency at www.ceop.police.uk/safety-centre. Reports are read by a Child Protection Advisor who will make contact by phone or email to work with you to make a plan to keep your child safe. If you think a child is in immediate danger, call the Police on 999 or NSPCC on 0808 800 5000.

SOURCES: Https://www.nspcc.org.uk/globalassets/documents/research-reports/how-safe-children-2018-report.pdf, https://www.telegraph.co.uk/news/2018/06/17/police-reveal-3000-sex-grooming-crimes-against-children-young, https://www.independent.co.uk/news/uk/crime/paedophiles-arrested-hundreds-police-warning-live-streaming-nca-online-dangers-uk-grooming-children-a8092851.html, https://www.nspcc.org.uk/what-we-do/news-opinion/Facebook-tops-list-online-grooming, https://projects.swan.ac.uk/onlinegroomingcommunication/

© National Online Safety Ltd
This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

www.nationalonlinesafety.com

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

A GUIDE ON HOW NOT TO BE A 'SCREEN ZOMBIE'

It's not always easy to tell if you've been spending too much time on your device. Mobiles phones, tablets, games consoles, TVs; the list of devices you might have access to seems never-ending and switching between them can be seamless. However, too much time on your device could lead to certain problems and could be an indicator of an addictive habit. It's important therefore that you try and manage your screen time as much as possible and avoid becoming a 'screen zombie.'

TAKE CARE OF YOUR BRAIN

Spending too much time on social media, watching YouTube or playing games online can result in you becoming a screen zombie. This can affect your mood, how much sleep you get, how you perform at school and how you behave around others. Limiting your screen time will keep you alert, Limiting your screen time will keep you alert, keep your mind focused and help to look after your own mental health and wellbeing.

BE PRESENT, NOT A ZOMBIE

Screen zombies often find that they spend a lot of time alone in front of their tablet or their mobile phone and reduce the time they spend with their friends or talk with their family. Zombies often lack communication skills. Always try to limit your screen time as much as possible – there's so much fun you can have with others!

SCREEN-FREE BEDROOMS

Keeping your phone in your bedroom means that it can be tempting to check every notification you get. Your phone could be the last thing you see at night and the first thing you see in the morning. This can contribute towards poor sleep and a lack of focus the next day. Try to keep your phone out of your bedroom or turn off all notifications before bedtime. This will mean you'll get a good night's rest and be ready for the next day.

CAUTION SCREEN FREE ZONE

DON'T GET TRAPPED INSIDE

Screen zombies usually find that they spend a lot of time inside as they lose interest in other things that don't include their device. It might seem obvious, but meeting your friends outside or doing outdoor activities like playing sports, trampolining, camping or just going for a walk are all healthy replacements for screen time and can help keep your mind fresh and active.

WARNING SCREEN ZOMBIES

ZOMBIE-FREE MEALTIMES

Mealtimes can be seen as a good time to sit down, relax and switch on your tablet or phone as you eat your food. But it can also mean that you're not interacting with others, sharing jokes at the dinner table or just talking about your day. Keep mealtimes for family time. Eating your food and staring at a screen means you're turning into a zombie.

BEWARE OF OTHER DANGERS

Spending too much time on your device and online can increase your chances of potentially encountering other online dangers. This could range from viewing inappropriate or harmful content to online bullying, grooming or fake news. Controlling how much time you spend online will reduce your risk of exposure. If you do see anything that makes you upset or if you're concerned about contact with others, always report it to a trusted adult.

BEWARE OF SNEAKY TRICKS

A lot of apps and games use certain ways of keeping you online and using their platform for long periods of time. This can include simple things like unlimited scrolling on a newsfeed, 'streaks' or uncovering hidden levels. Be mindful of how much time you're online and try to remember you're in control. You decide when you've had enough, not your device.

SAVE YOUR PARENTS!

Even though your parents will often be the ones telling you to limit your screen time, turn off your tablet or switch off your phone, sometimes they will forget to take their own advice. So it's up to you to make sure you remind them of the dangers of becoming a screen zombie!

ADULT SCREEN ZOMBIES AHEAD

UN-ZOMBIFY YOURSELF

If you think that you've already become a screen zombie, then don't worry, it's never too late to get help and support from your friends and family. Talk to your parents if you feel you've become addicted to your device, try to understand why and work with them to help you limit your screen time so that you can leave your zombie character behind.

SCREEN TIME 00:01

Meet our expert

Pete Badh is content specialist with over 10+ years in research and analysis. He has written various expert pieces around online safety for children and parents and previously worked in a specialist role for the police, contributing work which was pivotal in successfully winning high profile court cases and writing as a subject matter expert for industry handbooks.

NOS National Online Safety®

#WakeUpWednesday

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 17.06.2020

Live streaming is the term used to describe the broadcast of a real-time video from a mobile device, tablet or games console. Many live streaming apps have the functionality for interactions from viewers, such as commenting, live chats and sending reactions during the broadcast. Live streaming opens up a world of excitement for children, where they can watch live concerts, their favourite celebrities and bloggers/vloggers, connect with their friends, watch live gaming and much, much more. Whilst there are many positives with live streaming, it creates a worldwide platform for unsuitable content to be streamed and creates a host of dangers for children.

98% of child sex abuse live streaming victims are **13 or under**

IWF Internet Watch Foundation

LIVE

BIGO LIVE 13+ | Facebook 13+ | Instagram 13+ | Youtube 13+ | Periscope 13+ | Steam 13+ | Twitch 13+ | You Now 13+ | live.me 13+ | live.ly 13+

What parents need to know about LIVE STREAMING

SIGN UP PROCESS & AGE RESTRICTIONS

Most live streaming apps have the age restriction of 13 and above. It is important to note that some platforms do not require proof of age when signing up to the app, meaning that anyone can register an account. This also opens up the opportunity for people to lie about their age to seem older or younger.

RECORDINGS OF YOUR CHILD

Each streaming app and website that allows live streaming has different rules about how they store their live videos once completed. For example, a live stream on Periscope will be automatically deleted after 24 hours but apps such as Facebook and YouTube allow the video to be posted on the app afterwards and will only be deleted once the creator decides. It is important to know that deleting a video will not stop it from being shared. A live stream can be recorded (or screenshots can be taken) by other viewers using certain softwares and then shared on other platforms. According to research conducted by the Internet Watch Foundation (IWF), they found that the apparently recorded illegal videos of live streams were redistributed on other sites.

WHO IS WATCHING YOUR CHILD?

If your child's privacy settings are not set up effectively, anybody can be watching their live streams. One of the main characteristics of live streaming is its ability for videos to be instantly shared all over the world, but this creates the opportunity for more people to watch anybody.

WHAT IS YOUR CHILD WATCHING?

Live streaming apps don't just allow children to stream their own videos, they can also watch other people's streams. Anything can be streamed, at any time and any place, including violence, graphic imagery, nudity, illegal behavior, drug use, profanities etc. Most live streaming apps claim to monitor live streams and will take action to stop any that do not adhere to their guidelines. But, with millions of live streams each day, it makes it extremely difficult to monitor every one.

LIVE CONTENT

As the streams are live, children can be exposed to something inappropriate instantly. Most live streaming apps will have filters, rules and guidelines in place to ensure that their services are monitored. They will also have report buttons where inappropriate content will be sent for review. Keep in mind that a report may not be dealt with instantly which means your child will be further exposed to inappropriate content during a live stream.

GROOMING

There have been recent reports of paedophiles coercing children as young as 3 on live streaming apps. Due to the anonymous nature and lack of identification needed to sign up to some apps, almost anyone has the opportunity to sign up and use the service. Users can use fake identities to sign up to the apps and watch/stream videos. Recent research by the IWF revealed that children may be asked to do things and perform 'suggestive acts' during their live stream by strangers.

NOS National Online Safety

Top Tips for Parents

PROTECTING THEIR 'REP'

What your child does now may affect their future opportunities, and it is important that they have a good understanding of this. As the videos are live, it may lead to the misconception that whatever happens in the video will disappear once the live stream ends. This is incorrect. Talk to your child about how what they stream cannot be undone and has the potential to affect their online reputation.

REMOVE LINKS TO OTHER APPS

Some live streaming apps/websites give users the ability to link and share the content through other social media platforms to share their video further. For example, a live stream on Periscope, can be shared on Twitter and Facebook during the stream, if the accounts are connected. While this may seem like a good idea to show the video to more people, the privacy settings may differ on each app, opening up the opportunity for unwanted viewers to join the stream. We suggest checking the privacy settings on each app and where possible, only streaming on one app at a time to have more control over who sees the live stream.

TALK REGULARLY WITH YOUR CHILD

Ask your child what live streaming apps they are using and how they are using them. Are they watching live streams or making their own? What types of live streams do they like watching? If they are under 13, it is strongly advised that they are not using any live streaming apps due to the dangers involved, but you may feel that your child should not be using the apps even if they are over the age limit. With live streaming such a popular feature on apps, it is important that you are aware of the dangers associated with live streaming to effectively protect your child.

BE PRESENT

In a recent study by the Internet Watch Foundation (IWF) over a 3 month period, 96% of streams showed a child on their own, often in their bedroom or bathroom. If your child is going to conduct a live stream, ask them if you could be present for it. This will give you an opportunity and a better understanding of what your child is doing during their live streams and who they are streaming to.

PRIVACY SETTINGS

Each live streaming app will have its own privacy settings with options varying from platform to platform. Generally, we advise that your child's account is set to private. This will ensure that only their friends/followers will see their live stream. It is important to check each app to ensure that the privacy settings are in place to protect your child from strangers viewing their streams and engaging in conversation with them. Most apps settings will allow you to turn off the chat feature during a live stream, restricting conversations, but live chat is part of the 'fun' when it comes to live streaming.

PROTECT PERSONAL INFO

Your child may unknowingly give away personal information during a live stream, including their location. Talk to them about what constitutes as 'personal information' and make sure they do not disclose anything to anyone during a live stream, even to their friends. Advise them to remove any items in their live stream (school uniform, street name, posters etc.) that could potentially expose their location or information about them.

Sources

https://www.iwf.org.uk/ | https://www.pscp.tv/content | https://www.channel4.com/news/children-bombarded-with-sexually-explicit-chat-on-musical-ly-and-live-ly
https://www.independent.co.uk/news/uk/crime/paedophiles-child-sex-abuse-live-stream-direct-webcam-mobile-online-a8351986.html | http://www.bbc.co.uk/news/uk-44233544?utm_content=71916416&utm_medium=social&utm_source=twitter

© National Online Safety Ltd

This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

www.nationalonlinesafety.com

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

The latest digital trend growing in popularity for our children are apps on their phone or tablet that look like one thing but are secretly hiding another purpose. They first became particularly popular in 2016. However, children are becoming more and more familiar with 'secret' photo hiding apps, where an app which looks relatively ordinary is actually a hidden gateway to private photos and videos. These apps allow their users to hide images, videos and notes within the app which is also passcode protected. One of the most common types of hidden app used is a 'fake calculator' app however many others are also available.

What parents need to know about HIDDEN PHOTO APPS

MAY HIDE 'SEXTING'

The most common use for the apps is to hide 'sexting' images which young people may be sending or receiving. This problem is growing rapidly amongst students, and from an increasingly early age. Not only is sexting dangerous, but it is illegal when it involves a minor even if both the sender and receiver are underage. By storing and sending these images, young people should be aware that they are committing a crime.

PRIVACY RISK

If you are aware that your children are using the app, you should read the small-print in the usage policy/terms and conditions to ensure the developers do not have access to any of the images stored on the device. If the photos are linked to a cloud storage, then the images stored are also in danger of being released if the application is compromised/hacked.

ENCOURAGE IMPULSIVE BEHAVIOUR

Young people tend to act more impulsively if they believe that their behaviour will go unnoticed and remain secret, so often they will produce content for these apps thinking that it will be safe. Let's face it, how many adults read all the small print in the terms and conditions, so why would we expect our children to.

BYPASS PARENTAL CONTROLS

Although these apps are not specifically 'targeting' their advertisements towards children, they can generally be used by anyone over the age of 4. This means that these apps will not be blocked automatically by parental controls. Whilst online platforms, such as Apple, have removed these apps on numerous occasions from their app store, due to their popularity and potential profitability for creators, they continue to be produced and find their way into the stores or available for download.

FAKE/DECOY PASSWORDS

Some of the most secure apps that are available offer the ability to set-up a decoy feature as an added layer of security. This allows the user to provide a fake password which, when used, directs people to a decoy folder containing content of the user's choice or just stock photos. The real password provides access to the secret folder within the app.

National Online Safety®
#WakeUpWednesday

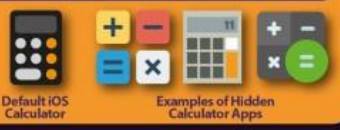
Safety Tips For Parents

TRY TO REMAIN VIGILANT

There is a natural human instinct to believe that what we see on screen is real and accurate. If you are concerned that your child might be using secret apps, you may want to look at their phone. The search feature on a device can be used to type keywords such as 'secret', 'hidden' and 'photo vault'. On iOS, this can be done by swiping down on the home screen to open a search bar. If the app appears and says 'Open' then the app is installed. If it says 'Get' then it is not installed. On an android device, you can go to the apps menu and use the search bar at the top of the screen.

QUESTION THE AUTHENTICITY OF DUPLICATE APPS

You should be aware that almost every mobile device will have pre-installed apps, such as notes and calculator, so the first major warning sign would be to look for duplicates of these apps. By default, the pre-installed apps are almost always displayed on the first page of the home screen.



DISCUSS THE DANGERS OF 'SEXTING'

Ensure your child is aware of the dangers of sexting, and how it is illegal to keep or distribute images of minors. Try to talk to your children in a positive way a nd encourage them to take control of their online persona and what they are posting to others. Remind them that they always have a choice and that they can say no to anything that makes them feel even the slightest bit uncomfortable.

LOOK OUT FOR IN-BUILT 'HIDDEN' FEATURES

iPhones have the option to lock notes within the default Notes app. Users can paste images into a note file and lock it using Touch/Face ID and a password. In addition, iOS allows their users to move images to a Hidden folder in the photos app. When an image is moved to the hidden folder, it is removed from the 'All Photos' folder. To find this folder, open the 'Photos' app, scroll down and click 'Hidden'. Users may also create folders to try and hide the app on their home screen or on a second or third page. If you see a folder on your child's device, ensure you check each page for hidden apps.

CONTROL APP USAGE

If your child's iOS device is linked to your Apple ID account, you are able to set a password for downloading apps which only you know. This will mean every-time your child tries to download an app, they will need your password to do so. If you do not have access to your child's Apple ID, you can delete the app without a passcode. This will delete any images stored on the app and will not be recoverable, even if the app is redownloaded.

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.

SOURCES: https://www.businessinsider.my/apple-pulls-private-photos-calculator-from-app-store-2018-4/, https://smartsocial.com/private-photo-calculator-app/, https://offspring.lifehacker.com/is-your-teen-hiding-sexting-photos-in-a-fake-calculator-1829529749

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 26.02.2020

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

Social media has its benefits for connecting with friends, sharing experiences and widening their understanding of broader issues beyond their local community. The challenge with connecting and sharing experiences via social media is that these shared experiences are often via images. Wanting to fit in and caring about their physical appearance is a perfectly normal part of adolescence. However, with the easy access of image changing software and filters, this physical appearance is often not the reality, further increasing the pressure for young people to gain or portray unreal perceptions.

What parents need to know about SOCIAL PRESSURES LINKED TO 'APPEARANCE'

ONLINE APPEARANCE AND MENTAL HEALTH

The opportunity to change physical appearance through social media apps is creating a high level of perfectionism for children to portray themselves faultless and compare themselves to images which are sometimes unreal. This can lead to anxiety, depression and poor self-image and an overall sense of never feeling good enough. Having poor self-image can affect the way that your child interacts with others and how we care for ourselves.

AIRBRUSHING

Refers to the retouching done to an image that changes the reality of the photo. It may include removing people, objects, altering body shapes or erasing blemishes like acne or scars. The digital technology to enable airbrushing is now widely and easily available for desktop computers and social media apps. It is sometimes known as 'Photoshop'.

FILTERS

Filters applied to manipulate a photograph are another way of creating a delusion of what is real. Software within social media apps reconfigure your face and skin to look more aesthetically pleasing. As innocent and fun as these filters may seem, they are sending a message that we are more attractive when our features are modified.

APPS WHICH CHANGE APPEARANCE

These relate to free downloadable apps or options within social media apps which create a fun and easy way to alter your appearance. They are designed to be fun and can become addictive because once an altered image is used, it is very difficult to revert back to an unaltered version of themselves.

MULTIPLE PHOTOS FOR THE PERFECT IMAGE

Taking multiple shots to capture the perfect image to put onto social media is another way of disguising reality. Creating an image which receives approval from peers through multiple comments and likes exacerbates the desire for a perfect picture and the approval for continuing to achieve the perfect image.

National Online Safety #WakeUpWednesday

Safety Tips For Parents

QUESTIONS TO CONSIDER BEFORE TALKING TO YOUR CHILD

- Do most of their social media photos have a filter/image changing app on them?
- How often do they talk about their physical image in a negative way?
- Do they often talk about wanting to gain comments and 'likes'?
- Are they excessively anxious about their physical appearance, to the point it impacts on their every day life?

If you have answered yes to most of these questions, then it would be a good idea to have a discussion about their use of image altering app's.

DON'T GO COLD TURKEY

Talk with your child about taking one unfiltered image of themselves and sharing it with family first and then posting on social media. Perhaps ask other members of the family to send or post on social media unaltered pictures of themselves.

BE COMPLIMENTARY

Whilst improving body image starts with the child's image of themselves, complimenting them daily on their personality and qualities will provide external, positive encouragement about themselves, away from just their physical appearance.

DAILY APPRECIATION

When we have the sense that we are not good enough, we can feel like we are always falling short. You and your child together might want to create a gratitude journal, board with post-it's or wipe board where you write down things that you are grateful for or appreciate. This could range from the weather to a kind deed or to a piece of work that went well.

CHANGE THE STORY

We all have a narrative or a story we've created about ourselves that shapes our core self-image. Sometimes automatic negative thoughts like 'you're fat' or 'you're ugly' can be repeated in your mind so often that you start to believe they are true. These thoughts are learned, which means they can be unlearned. You can start with helping your child reframe the story into a more positive assertion or story. This will link to complementing and daily appreciation.

WHEN TO GET HELP

If your child becomes overly despondent, withdrawn or there is a change in behaviour over a prolonged period of time, they may need some professional support to help them.
https://www.bacp.co.uk/search/Therapists
https://www.themix.org.uk/ is good organisation as a source of support if your child wants to reach out for support themselves

Meet our expert

Anna Bateman is passionate about placing prevention at the heart of every school, integrating mental wellbeing within the curriculum, school culture and systems. She is also a member of the advisory group for the Department of Education, advising them on their mental health green paper.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 18 .09.2019

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

Personal data is a strange commodity. Cyber thieves can buy huge quantities of personal data on the black market for very little, yet your own personal data is hugely valuable to you. If your personal data falls into the wrong hands, it could lead to identity theft, bank fraud or something even more sinister such as stalking. The severity of that threat is multiplied when it comes to the personal data of children, when threats such as internet grooming begin to emerge. The bad news is that children aren't always great at safeguarding sensitive information, which is why they need parents' help and guidance. That's why we've created this guide to show you how you can protect your own and your family's personal data.

What parents need to know about PROTECTING PERSONAL DATA

EVERY DETAIL IS KEY

Which info should you be wary of sharing online? Aside from the obvious, such as full names, date of birth and address, think of the type of information you're asked for when answering security questions for services such as online banking. The name of your first school, your mother's maiden name, the names of your pets, your favourite band. Data thieves will harvest as much of this information as possible, so don't make it easy for them by publishing it anywhere online.

SOCIAL MEDIA VISIBILITY

Social media sites, such as Facebook, encourage us to share sensitive information in order to build our online profiles. Many people are lulled into thinking that only their friends can see such information, but that's rarely the case. Such information can easily be shared with 'friends of friends' or even anyone searching for you online because privacy settings are opaque. Keep social media profiles to the bare minimum. If you wouldn't be comfortable hanging a sign with that information on your front door, don't enter it into social media sites.

DANGEROUS GAMES

Online games are a particular risk for children. Many of the most popular games – such as Fortnite, Minecraft or Roblox – have voice or text chat facilities, allowing them to talk to fellow gamers. Or, sometimes, people pretending to be fellow gamers. It's very easy for children to be seduced into divulging personal data such as their address, birthday or school. It's critical parents both educate children on the dangers on online chat in games and take safeguards to protect children.

IMPOSTERS AND PHISHING ATTACKS

Even if you're scrupulous about keeping your data private on social media, it's easy to be lulled into handing it over to imposters. There are two golden rules for you and your children to follow: 1. Never divulge personal information to phone callers, unless you can be absolutely certain you know who they are. 2. Never click on links or open attachments in emails or social media, unless you're 100% certain they are genuine. So-called phishing emails are growing ever-more sophisticated, with fraudsters able to replicate the exact look of bank emails and even include details such as account numbers and IDs.

THE RISKS OF PASSWORD SHARING

Password sharing – using the same password for multiple sites – is one of the easiest ways to lose control of your personal data. Hacking of major websites, including usernames and passwords, is common. If you're using the same password for a hacked site as you do on your Gmail account, for example, you're handing data thieves an easy route into your inbox, where they will doubtless find all manner of sensitive information, such as bank emails and contacts. Your email account will often also let them reset the password on multiple other accounts. Don't share passwords; use password managers to create strong, unique passwords for every site.

National Online Safety®

#WakeUpWednesday

Safety Tips for Parents & Carers

LOOK OUT FOR LEAKS

Many security software packages have features that look for personal data leaks or prevent people from entering it into risky sites in the first place. For example, Bullguard Premium monitors dangerous sites for usage of data such as your email address, debit card numbers, passport number and more, and then sends you email alerts and details of how to take remedial action if it spots them being used. Such software also issues warnings if it sees personal data being entered into unprotected, high-risk sites.

KEEP DATA GUARDED

Don't give the thieves a head start by handing them pieces of sensitive information for free. For example, it's very common to see email address such as davesmith1976@gmail.com – an immediate clue that you were born in that year. If you have a less common name than Dave Smith, thieves could immediately start using that information to cross reference against public records or other database breaches, allowing them to start building a profile of information about you. Likewise, don't use your date of birth in a password. If that's hacked, you've handed the thieves another big clue.

DON'T OVERSHARE ON SOCIAL MEDIA

The biggest threat to your child's privacy is you. Parents often overshare personal information on social media: full names, names of schools, children's birthdays, names of their friends. All of this can be easily gleaned to build profiles that could be used to groom your child in online games or in real life. Exercise extreme caution with social media posts concerning your children.

BE WARY OF SHARED NETWORKS/SYSTEMS

Avoid entering any personal data into a web browser when you're using public Wi-Fi (in a coffee shop or airport, for example) or when using shared computers. Shared Wi-Fi connections are much easier to eavesdrop on than your home network, especially if they are not password protected or the password is shared freely with customers. Don't do online shopping, banking or enter any logins/passwords when using shared Wi-Fi. Likewise, if you're using a shared computer at work, for example, as it's very easy for a browser to save logins that could be used by others.

PLAY SAFE IN ONLINE GAMES

Children must be taught to treat strangers in online games with the same caution as they would treat strangers in the street. Don't allow children to use their real name as their username in games to prevent imposters conning kids into thinking they are real-life friends, and only allow them to add friends in the game that they know in real life. Regularly ask to monitor your child's friends list in such games and ask them to identify who the players are. With younger children in particular, ask them to only use voice chat in family rooms, so that you can hear conversations.

Meet our expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as *The Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *BBC Newsnight*, *Radio 5 Live* and the *ITV News at Ten*. He has two children and has written regularly about internet safety issues over the years.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.07.2020

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one online risk 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 need to know about VPNs

Although a great privacy tool in the right hands, VPNs can be dangerous for children and let them bypass restrictions you have on web browsing.

What is a VPN?

A Virtual Private Network (VPN) is a privacy tool used to hide internet activity from prying eyes. Without a VPN, internet traffic is sent directly from your computer or smartphone, letting anyone in-between you and a website or service that you're accessing (such as a wireless hotspot owner or your ISP) see what you're doing. With a VPN, a secure tunnel is created between your computer or phone and what's known as the endpoint. The endpoint is merely the part of the internet where your connection comes out and can be in the same country as you or located anywhere else in the world.

Using a VPN has two main effects. First, as the tunnel is fully encrypted, nobody between you and the final endpoint can see what you're up to. Secondly, as all of your traffic looks as though it's coming from the endpoint, you can further avoid being tracked and monitored, hiding your real location from everyone.

VPNs have many legitimate uses. For example, running a VPN when on a wireless hotspot or hotel network that you don't trust, gives you additional security. There's also improved privacy by using a VPN, preventing ad networks and the like from tracking you and working out where you live. VPNs are also often used to bypass protections, say watching UK streaming TV when abroad by pretending that you're still in the UK.The way a VPN works means that children can also use VPNs to hide what they're doing and get around any restrictions that you might have in place.

National Online Safety®

Publish date: 20/03/19

MEET OUR EXPERT

This guide has been written by David Ludlow. David has been a technology journalist for more than 20 years, covering everything from internet security to the latest computing trends and the smart home. A father of two (a nine-year-old and a six-year-old), he's had to control and manage how his children access online services and use apps.

What are the risks?

There are three main issues with VPN usage by children, potentially affecting their privacy (and yours), and opening them up to seeing inappropriate content.

1) Viewing age-inappropriate content

Parental control tools work by looking at the sites that a child is trying to visit, and then blocking according to a list of what's not allowed. With a VPN, the secure tunnel that's created means that web traffic can't be viewed, so parental controls stop working. Once on the open internet, a child using a VPN can look at anything they like unrestricted. This isn't just at home. Children that are allowed to take devices into school for work purposes can also use VPNs to bypass any filters that have been set up on the school network, too. VPNs can both be in software and via what's known as a proxy website. With a proxy website, a child visits this, then enters in a blocked website address that they want to view. the blocked website is then downloaded and viewed through the proxy, sidestepping any parental protection.

2) Malware infections

Installing any unknown application is fraught with danger, and the same applies to many free VPN applications. In an investigation, it was found that 38% of free Android VPNs contained malware, with 75% also designed to track activity. By installing suspect software, a child may be opening themselves up to being spied on and their private details being stolen. If you use a shared device with a child, an infection can also affect you. Malware can spread, and there's then a higher risk to other devices on your network. There's a chance that a dodgy VPN will use your computer and internet bandwidth, too. Back in 2015, the free Hola VPN extension was found to be secretly selling its users' bandwidth via another service and, in some cases, users' internet connections were being used for illegal activity.

3) Free VPNs can spy on people

The best commercial VPNs are built around privacy and have strict rules about hiding activity, not spying on users and not logging data. These tools are built for adults who wish to protect their anonymity. Children often go for free VPNs and proxy websites, which have a less strict code of ethics. Many free VPNs have been found to spy on activity, store private information and even sell this data on. When using a VPN like this, dodgy adverts and pop-ups can be inserted into web traffic, beyond the harmful things that your child may already be viewing.

What parents can do

Although the risks might seem entirely different, the protection from VPNs is the same for all of the threats.

OFF
ON

Filter VPN sites

Check the parental controls software that you're using to see if there's a filter to block VPN/Proxy traffic. If this is selected, it will prevent most known VPNs from working, along with proxy websites.

Block VPN applications

Stopping and removing any VPN applications running on a child's device is a must. If you have parental control software that can restrict application use, make sure that you investigate any application that your child wants to install and block all VPNs. If you've recently enabled any applications, go back and check what they're used for and remove any VPNs that you find. If you don't have software to check what's running on a child's devices, then you should manually check. Searching for an application with VPN in the name is a good idea. Look out for tell-tale signs, too: computers and phones will usually display a different connection symbol when a VPN is connected. You can also use a child's computer to try and view a restricted website to ensure that filtering is still in place.

Monitor your child's online activity

In order to prevent your children from falling prey to inappropriate content, it's important to monitor your child's internet usage and have open and honest discussions with them about their online activities.

Sources:
www.safenet.com/blog/use-free-vpn-hola-risks-cybercrime/
https://research.cnb.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf
www.pcworld.com/article/2920340/ultra-popular-hola-vpn-extension-sold-your-bandwidth-for-use-in-a-botnet-attack.html

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 20.03.19

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

Understanding Video Game LOOT BOXES & SKIN BETTING

ONLINE GAMING

Much is written in the media about online gaming, gambling and "skin" betting. These terms can be confusing as they mean different things in different contexts. Online gaming has historically meant gambling websites with cards, slot machines and roulette. More recently, as we are discussing here, online gaming has also come to mean video games you play over the internet. In online video games, players can often start playing for free. As they progress, the game offers in-app purchases that provide equipment, weapons, outfits and enhancements to characters. These are usually small purchases of just a few pounds. However, games offer many hundreds of these purchases that can mean children spend a considerable amount of money.

LOOT BOXES

Some video games also offer what has been called "loot boxes" as a way to purchase these items. Similar to purchasing a pack of Panini football stickers or a Lego Minifigure in foil packaging, players don't know exactly what they will get. They may get a common item that has a low value in the game. Equally, they may get a rare item that has a high value. These interactions are not considered to be gambling according to the UK Gambling Commission, although sometimes they have a similar appearance because the items obtained have no monetary value outside the game. Only games that contain simulations of real-world gambling have the PEGI Gambling descriptor. However, games that offer in-app transactions of any kind are flagged with the PEGI In-App Purchase descriptor on the box or at point of sale online.

SAFE SETTINGS

It's important that parents try this out with children as they venture into the world of gaming. Together they can build an understanding of how these purchases work and discuss which are really good value, and which are over-priced. Like pocket money, it can be a good way to teach children about virtual currency and online purchases.

It's important to understand that it can be easier to make repeat purchases online compared to buying toys or stickers over the counter. Also, many games offer high-cost top-ups of virtual currency (up to £79.99) in a single purchase. While these are sometimes labelled "best value" they represent a significant investment in a game that should be considered carefully before purchase.

It's worth noting that Microsoft, Sony and Nintendo have agreed to disclose the odds of getting rare items in loot boxes. Game publishers on these platforms will have to reveal the chances of each purchase. Some publishers do this already. Together with your child, you can set-up spending limits to stop accidental purchases. A good approach is to use the pocket money feature on consoles to allow them to spend a small amount each month. You can also avoid putting your credit card details in by using pre-paid cards that work like book tokens. If you do add credit cards ensure you set up a password on the account.

National Online Safety®
#WakeUpWednesday

SKIN TRADING

Because players can trade and swap items in games, the relative rarity of these items creates a thriving market where these items are exchanged. This trading aspect of games like Rocket League can be an enjoyable way for players to get the items they want, similar to swapping football stickers in the playground.

Because these items are often just visual changes to how characters look they are called "skins", although, in reality, this includes items that do more than change appearance. It's important for parents to understand that these "skin" trades are often arranged on websites or apps outside the game itself. This can mean that parents are unaware of trades. Also, the third-party communities are unregulated and beyond the control of the game creator.

SKIN BETTING

Use of this "skin" currency can be taken further by websites that use it for gambling. "Skin betting" is when players use these virtual items they have earned or purchased in games as gambling currency. Players can also use these sites to bet with "skins" on eSports competition outcomes. It's important for parents to be aware of this activity, as it can consume considerable amounts of money if a player is buying in-game items for this purpose.

Where this becomes a legal issue, is when the "skins" you win can be converted to cash. As the Gambling Commission stated in its Young People and Gambling 2017 Report, "Where gambling facilities are offered to British consumers, including with the use of in-game items that can be converted into cash or traded (for items of value), a gambling licence is required."

In particular, this means that these sites must not be accessible or advertised to children. "Tackling operators making gambling facilities available to children is one of the Gambling Commission's priorities. This has been demonstrated by action taken against unlicensed websites providing facilities for gambling using in-game items as methods for payment." Along with the Gambling Commission, the games industry strongly opposes "skin" betting sites as they infringe the legal agreements that underpin games. Games companies work with law enforcement agencies to clamp down on these sites.

VALUING IN-APP PURCHASES

Understanding how modern games make money enables you to guide your family to find the best value in the games they play. Whether it's taking advantage of the many free to play games now available, making informed decisions about in-app purchases or spending weekend pocket money after a hard week at school, this way of paying for games can work.

Meet our expert

Andy Robertson is a parent of three children and journalist who writes for national newspapers and broadcast television. His Taming Gaming book helps parents guide children to healthy play.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 02.10.2019

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

"The industry, as far as we can see as families, are grooming the next generation with a whole set of online games and these are aimed at 7, 8, 9 year olds – that's the next generation who are going to be their income generators" - Liz Ritchie, Gambling With Lives

The digital world that we live in can be a minefield for families and parents/carers. The way in which children 'game' now is completely different to how modern day parents and carers would have experienced. The 'monetization' of gaming is at the forefront of research and there are increasing concerns surrounding online gaming and the subsequent links this has with underage gambling.

From ONLINE GAMING to ONLINE GAMBLING

Recognising the Signs

10 Signs for Parents to Look For:

Disordered gambling is sometimes referred to as the 'silent killer'. Unlike drug or alcohol addictions the signs are sometimes harder to spot and if not dealt with at an early age can have a devastating affect on both the gambler and their families later on in life.

1 EXCESSIVE USE OF DEVICES

This can lead to increased isolated behaviour and lying about the amount of time spent online.

2 SPENDING MONEY ONLINE WITHOUT PERMISSION

If a child is willing to spend money online (invariably on a parent's card) without permission then this should act as an eaarly warning sign to parents to ensure that there are some barriers and parental controls in place.

3 CHANGES IN BEHAVIOUR

Children may become moody, aggressive or argumentative particularly during or shortly after periods of online gaming.

4 A CHANGE IN ATTITUDE TO SCHOOL

Children may display an obvious change in attitude to learning and a more negative view of school.

5 DISENGAGED WITH FAMILY LIFE

Children start to prefer spending time alone online rather than engage in normal family activities.

6 COMPULSIVE EATING

This includes both eating the wrong types of food excessively and not eating healthily.

7 IMPATIENT

Not prepared to wait for anything (mirrored in excessive online game play and in app purchases) and nothing is ever good enough.

8 'THE LOOK'

Compulsive gamblers are often said to look zoned out, have a greyness, look ill, experience a loss of weight and stop taking pride in their appearance. The same can be said of those who are starting to develop a gaming addiction.

9 OBSESSIVE BEHAVIOUR

Children who demonstrate obsessive behaviour in everyday life are often reported to be 'at risk' of developing an online gaming disorder.

10 DISHONESTY

This could include starting to tell lies and in the more extreme cases even stealing things.

10 Top Tips for Parents:

If you think that your child may be at risk of developing a gaming addiction then there are a series of measures that you can put in place. This is by no means an exhaustive list but just some strategies that could ensure a potential situation does not escalate.

1 BE AWARE

Do not fall into the trap that it's just what children do – as parents/carers/families be 'on the same page' and do not be allowed to be played off against one another.

2 VISIT THE GP

Although both gaming/gambling addictions are now recognised as a mental disorder, some doctors may not be experts in these areas – families can self-refer to NHS Gaming and Gambling Clinics.

3 DO YOUR RESEARCH

See what help and support is available. Visit www.gamfam.co.uk and become an expert.

4 SPEAK TO THE SCHOOL

Have an open and honest conversation. Schools are investing heavily in mental health and can arrange or direct you to the most appropriate support services.

5 TAKE AN ACTIVE INTEREST

This applies to school work and in creating a learning environment at home. Find activities and hobbies that create a life away from the screen and be part of it.

6 BECOME THE EXPERT

Research the game your child is playing – does the game have loot boxes?

7 PUT BARRIERS IN PLACE

Set up parental controls for all devices (including phones) and set up screen time. Visit the 'Partnership with Parents' section at www.gamfam.co.uk for further details.

8 FINANCIAL CONTROLS

Turn off in-app purchases. Do not link your debit/credit card to your child's device and use a prepaid card instead. For example Monzo, Go Henry, Nimbl or speak to your bank for advice.

9 DISCUSS LOOT BOXES AND SKIN BETTING

Have a conversation about loot boxes and skin betting. Many games can still be played and completed without using loot boxes on the console version but be mindful of the mobile versions.

10 DO NOT LEND MONEY FOR GAMBLING

Or if you think it will be used for online gaming, without your permission.

National Online Safety®
#WakeUpWednesday

The above guidance has been produced by GamFam

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 12.02.2020

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

SOCIAL MEDIA & Mental Health

What trusted adults need to know

Social Media is often scrutinised as having a negative impact on children's mental health. Whilst currently there is not enough evidence or research to say whether this is true or not, there are certain 'modern pressures' connected with social media which trusted adults need to be aware of. Children and young people are constantly connected and whilst this comes with some benefits, it also comes with a feeling that you are constantly visible. This guide is designed to encourage trusted adults to think about their children's mental health and their social media activities, providing them with some useful tips on improving and supporting mental health among young people.

Five potential signs & symptoms of mental health difficulties

1. Have you noticed a change in your child's personality? They may not be acting or feeling like themselves.
2. Any recent uncharacteristic anxiety, anger, or moodiness?
3. Is your child experiencing social withdrawal and isolation?
4. Is there a sudden lack of self-care or risky behaviours?
5. Does your child have a sense of hopelessness or feel overwhelmed?

National Online Safety®

#WakeUpWednesday

1. EDUCATE YOURSELF

Educate yourself about social media sites your child is using so you can really understand what they are experiencing and how this may be making them feel.

2. DISCUSS REAL-LIFE CONNECTIONS

Talk about the importance of face-to-face time with friends and family, and what enjoyment this can bring. Encourage your child to focus on their relationships with people who make them feel good about themselves.

3. SUGGEST REGULAR BREAKS FROM SOCIAL MEDIA

Encourage your child to take regular breaks from checking their social media platforms. You could suggest that they turn off their app notifications during certain times of the day so they can focus on other things.

4. ENCOURAGE OTHER HOBBIES OR INTERESTS

Spending time away from their phone and devices will offer them an opportunity to discover other interests and activities they may enjoy. This could be sports, playing a musical instrument or creative interests such as arts and crafts.

5. OFFER YOUR SUPPORT

Inappropriate and harmful content can be accessed on the internet which may impact your child's mental health. Explain to your child that not everything online is real and ensure they know that you are there to support and advise them about any worries or anxieties they may have.

HELPFUL APPS:

- Hub of Hope
- Mindshift
- Smiling Mind

OTHER SERVICES:

- Childline (0800 1111)
- Bullying UK (0808 8002222)
- Young Minds (0808 802 5544)

Meet our expert

This guide has been written by Anna Bateman. Anna is passionate about placing prevention at the heart of every school, integrating mental wellbeing within the curriculum, school culture and systems. She is also a member of the advisory group for the Department of Education, advising them on their mental health green paper.

Sources: https://www.centreformentalhealth.org.uk/publications/social-media-young-people-and-mental-health, https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/articles/measuringnationalwellbeing/2015-10-26, https://www.rsph.org.uk/uploads/assets/uploaded/62be270a-a55f-4719-ad668c2ec7a74c2a.pdf, https://www.psychologytoday.com/us/blog/cutting-edge-leadership/201505/5-warning-signs-mental-health-risk

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 15.05.2019

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

SUPPORTING CHILDREN'S MENTAL HEALTH

10 Conversation Starters for Parents

Talking about mental health to children is sometimes hard. To the point that we can put off raising the subject, not wanting to unearth problems or raise overwhelming subjects that we perceive our child is too young or not ready for. But rather than keeping children in the dark, this guide is designed to help you confidently talk about mental health, so they feel comfortable talking about their own worries and end any stigma before it begins.

National Online Safety®

#WakeUpWednesday

1 LISTEN

This sounds obvious, but it is not something we are always great at. Active listening is where we listen without interrupting or making judgements and shows interest in what is being said. If your child feels listened to in the 'smallest of problems' they will become confident that you will listen when the 'biggest of problems' arise.

2 ASK TWICE

The campaign from time to change is great . https://www.time-to-change.org.uk/support-ask-twice-campaign. Be tenacious about your child's wellbeing. Children instinctively know when your questions and support come from a place of wanting to help and care.

Are you sure?

3 THERE IS NO SUCH THING AS A STUPID QUESTION

This advice also relates to the first point. If your child can ask you any questions about the smallest of things and you listen and answer without shaming or belittling, then they will have more confidence to ask the biggest of questions.

4 BE OPEN AND HONEST

Children appreciate honesty, particularly if you are having to share information or talk about a difficult subject. For example, you may be talking about death or loss; 'It's very sad that Nana has died' or 'I feel sad that Nana has died'. How you talk about a subject will differ depending on their age and developmental maturity. Talking about death to a younger child for example will be different to that of an older teen, as their experience and understanding of death is different.

5 KNOW WHEN TO SEEK HELP

Assess the severity of the mental health difficulty you are noticing. Is the difficulty making it hard for your child to function regularly throughout everyday life? How frequently is your child affected, how long does it last and how persistent is it? Are they having problems controlling the difficulty? Talk to your child about your concerns and that it is likely they will need further support beyond family and friends.

6 TALK ABOUT MENTAL HEALTH NATURALLY

Speak about mental health as part of everyday life, so that talking about our feelings and those of others is normalised. If the usual 'are you ok?' is not creating an opportunity for dialogue then say something like 'I know when something like that has happened to me I felt like this… is that how you are feeling or are you feeling something else?'

7 EMPATHISE

'It makes sense that you would feel this way, it is understandable'. Children often worry about things that we, as adults, might see as trivial or silly. However, for them at their age and stage it is a big concern and they need our kindness and care when they show their vulnerability and share their worries.

8 HELP YOUR CHILD FEEL SAFE

Teens particularly feel that by talking about their worries or concerns that this will make things worse. Reassure your child that you will discuss a plan of action together and what may or may not need to happen next. If they are a younger child, it is likely you will need to lead the conversation and explain next steps.

9 MIND YOUR LANGUAGE

Be mindful of the language you use at home to describe and talk about mental health. Stigma often arises from misconceptions and a choice of language which is harmful. Using the word 'mental', 'man-up' or other such words in a derogatory way won't encourage your child to talk about their mental health for fear of being belittled.

%!#&

10 IT IS OK TO SAY 'I DON'T KNOW WHAT TO DO NEXT'

Adults do not have all the answers but often children think they do. It is ok to acknowledge that what your child is experiencing is not something you have come across before or know anything about, but that you will work it out together and seek help together.

Meet our expert

This guide has been written by Anna Bateman. Anna is passionate about placing prevention at the heart of every school, integrating mental wellbeing within the curriculum, school culture and systems. She is also a member of the advisory group for the Department of Education, advising them on their mental health green paper.

Sources of Information and Support

Your GP
Young Minds https://youngminds.org.uk/v
https://www.nhs.uk/conditions/stress-anxiety-depression/
https://www.actionforchildren.org.uk/news-and-blogs/parenting-tips/2016/november/a-simple-guide-to-active-listening-for-parents/
https://www.themix.org.uk/mental-health

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 05.02.2020

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

National Online Safety®

#WakeUpWednesday

Online Safety Tips For Children

Do's

1 KEEP YOUR PERSONAL INFORMATION PRIVATE ONLINE

Only share it with people you know like friends and family. Ask a trusted adult, like your teacher or a family member, to help you change your privacy settings so that strangers can't see it.

2 SPEAK POLITELY AND BE KIND TO OTHERS WHEN YOU SPEAK TO THEM ONLINE

Treat them like you would treat them in real life and always remember your manners.

3 TELL A TRUSTED ADULT IF YOU ARE BEING BULLIED ONLINE

If other another person is sending you nasty messages, a trusted adult will be able to help you collect evidence and report the person to the relevant authorities.

4 USE PASSWORDS TO PROTECT YOUR PERSONAL INFORMATION

Ask a trusted adult to help you create a password that you can easily remember but which is hard for other people to guess.

5 ALWAYS CHECK WITH A TRUSTED ADULT FIRST BEFORE USING A DEVICE OR DOWNLOADING A NEW APP

This is so that they can check it is safe for you to use and make sure the privacy settings are right.

6 TELL A TRUSTED ADULT IF YOU SEE SOMETHING ONLINE WHICH YOU DON'T LIKE

This can include anything that upsets you, makes you feel sad or which you're unsure about.

7 USE THE INTERNET TO HAVE FUN AND TO HELP YOU FIND OUT INFORMATION ABOUT THINGS

Remember to ask your trusted adult for help and always use child friendly search engines so that the information you get back is safe.

Don'ts

1 ACCEPT FRIEND REQUESTS FROM STRANGERS OR PEOPLE YOU DON'T KNOW

Always tell a trusted adult if somebody you don't know tries to contact you online.

2 SPEND TOO MUCH TIME ON YOUR DEVICE

Instead, go out and play with your friends, get some fresh air and try to exercise more. This will help you stay fit and healthy.

3 REPLY TO MESSAGES FROM ONLINE BULLIES OR PEOPLE WHO SEND YOU NASTY MESSAGES

The most important thing to do is to tell a trusted adult and then block the person from contacting you.

4 COPY PEOPLE'S WORK ONLINE OR PRETEND IT IS YOURS

BY AHMED

BY OSCAR

This is called plagiarism and can get you into a lot of trouble.

5 BE MEAN OR NASTY ONLINE

%!#&

Behave online like you would in real life and don't post anything that can make you look like a bad person. Things that you post online can stay there for a very long time.

zZZ

6 USE YOUR DEVICES CLOSE TO BEDTIME

This will allow your brain to rest so that you can get a good night's sleep, stay focused at school and perform better in class.

7 SHARE PERSONAL INFORMATION ON THE INTERNET WITH STRANGERS

Always tell a trusted adult if somebody you don't know asks you for your personal information.

%!#&

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 27.11.2019

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

National Online Safety®

#WakeUpWednesday

14 WAYS TO BE KIND ONLINE

Showing kindness online can mean so much to someone else. It is a choice we can all make that helps others, puts people's needs before our own and which can generate feelings of empathy and compassion. Small gestures can have a large impact and often one act of kindness can lead to more, making the world a happier and more positive place. That's why we've created this guide to suggest a few simple 'acts of kindness online' that can benefit people's mental health, support their wellbeing and encourage a more positive approach to engaging online.

1. BE POSITIVE

Post about things that make you happy and that you're thankful for. It could brighten up someone else's day.

2. OFFER TO HELP

Sometimes a friend or family member might post a question online or ask for help with something they can't do themselves. If you know the answer or are able to offer help, provide support and send a response. Something that may be easy for you might be difficult for someone else.

3. SHOW APPRECIATION TO OTHERS

If somebody you know has done something good or shown kindness themselves, thank them for it. It costs nothing and showing them that you appreciate it means so much.

4. SHARE FUNNY VIDEOS OR IMAGES WITH FRIENDS & FAMILY

We often come across funny videos or images online that make us laugh and then we move on. If you found it funny, your friends and family might too. It could help someone smile who may be having a bad day.

5. LIKE, LOVE & CELEBRATE

If somebody posts something that you like on social media, like it, love it or celebrate it! It's a small gesture but could mean a lot.

6. VIDEO CALL YOUR FRIENDS & FAMILY

It can be easy to be consumed by daily routine. Using apps like Zoom, FaceTime or WhatsApp are great for connecting with others far away and shows you're thinking of them even though you can't physically meet them in person.

7. TELL SOMEONE YOU'RE THINKING OF THEM

We can't always tell how people are feeling online and just dropping somebody a message to ask if they're ok or that you're thinking of them could literally make their day.

8. SHARE POSITIVE POSTS

If you see something online that inspires you, share it with people you know. An inspirational quote, a beautiful photo or a motivational video can lift spirits, improve self-esteem and help make people feel better about themselves.

9. HOST AN ONLINE QUIZ

Video conferencing apps are a great way to get friends and family together. If you know someone who is feeling lonely, host an online quiz and invite them to join in. It could really cheer them up.

10. THINK BEFORE YOU COMMENT

Sometimes thinking before you act can be just as significant as acting in the first place. Showing thought before you comment could stop you posting something hurtful, offensive or negative. It's always better to post positively or post nothing at all.

11. BE COMPASSIONATE & UNDERSTANDING

Being empathetic towards others and their situation is often an act of kindness and selflessness that gets overlooked. If you notice someone who is upset, drop them a message and offer to listen.

12. CONNECT FRIENDS & FAMILY WITH SIMILAR INTERESTS

You may know two people amongst your friends and family who you trust and know well who have similar interests and likes. Introducing them can be a great way for them to make new friends but remember to always ask their permission first.

13. RECOMMEND SOMETHING YOU ENJOY DOING TO OTHERS

If you enjoy doing something online, such as playing a game, or if you've found a great learning resource, share it with others. Even if you've watched a good film, letting others know can be an act of generosity that brings them excitement or pleasure at a time when they might need it the most.

14. PRAISE OTHERS FOR THEIR ACHIEVEMENTS

Sometimes your friends or family might post something online that they're proud to have done. It might be an exam they've passed, learning a new skill or just completing a task. Either way, it's always kind to recognise hard work and effort through praise and celebration.

Meet our expert

This guide has been written by Anna Bateman. Anna is passionate about placing prevention at the heart of every school, integrating mental wellbeing within the curriculum, school culture and systems. She is also a member of the advisory group for the Department for Education, advising them on their mental health green paper.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 20.05.2020

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 issue 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 TIKTOK

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

AGE-INAPPROPRIATE CONTENT

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

18

CENSORED

EXPLICIT SONGS

W&#*!

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

TIKTOK FAME

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

IN-APP SPENDING

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

Advice for Parents & Carers

TALK ABOUT ONLINE CONTENT

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

MAINTAIN PRIVACY SETTINGS

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

LEARN ABOUT REPORTING AND BLOCKING

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

ENABLE FAMILY PAIRING

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

USE RESTRICTED MODE

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

MODERATE SCREEN TIME

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

Meet Our Expert

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

National Online Safety

#WakeUpWednesday

SOURCES: www.tiktok.com

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 27.10.2021

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

Edit date: 29/05/19

AGE RESTRICTION 13+

Snapchat is a photo sharing app for mobile phones and tablets. The app allows users to share images, videos and chat with friends through voice call or text message. Users can share images and videos directly to specific friends, or through a 'story' shared with their entire friend list, which documents the previous 24 hours. In a study, Snapchat was ranked the 4th most negative app in terms of having an impact on young people's health and wellbeing, with children feeling that they can use the app Snapchat to "make you look pretty."

What parents need to know about SNAPCHAT

EXPOSING YOUR CHILD'S EXACT LOCATION

The 'Snap Map' lets you share your EXACT location in real-time through a map on the app. The user's location updates when the app has been opened on the device. There is a warning on the Snapchat website about uploading images and videos to 'Our Story' stating that "snaps you submit to 'Our Story' can still show up on the Map, no matter which location setting you choose!." When uploading to 'Our Story,' your child's image or video could appear in "Search results and Stories on or off Snapchat - today or in the future."

ADDICTIVE SNAPSTREAKS

'Snap Streaks' are gained when snaps have been sent back and forth consecutively between friends. The longer that snaps are sent between users, the longer the streak becomes. Furthermore, Snapchat rewards users who have achieved high Snap Streaks, by gifting emojis, adding incentives for users to keep the streaks. Children invest time into making their streaks as long as possible, which can put an incredible amount of pressure on both themselves and their friendships.

SEXTING

While Snapchat's gimmick is that all photos, videos and text disappear eventually, users still have the capability to screenshot or record anything which has been sent to them. Users may sometimes forget that screenshotting is possible and send a compromising image or message to somebody who they think they trust. Due to 'Snaps' disappearing, (users can even send a one-second photo or video), Snapchat has become the chosen platform for children and young people to send sexually explicit images or 'selfies.' Once a photo/video has been screenshotted, or recorded using another device or software, this can lead to further dangers, such as blackmail and cyberbullying.

It is illegal to make, possess, download, store and share sexual images, photos and videos of a person under the age of 18. This also includes any sexual images, photos and videos that a child may have taken of themselves. However, if a young person is found creating or sharing images, the police can choose to record that a crime has been committed, but taking formal action isn't in the public interest.

EXTRAS TO MAKE YOU STAY

Aside from taking photos and videos, Snapchat has other elements to keep users coming back for more. 'Snap Games' is a feature within the app where users can play minigames with others on their friends list. The games function is easily accessed by tapping on the rocket button during a conversation. Another feature on the app is 'Snap Originals', which allows users to watch content created by Snapchat, celebrities and other accounts, including a mixture of comedy shows, drama, news and more. These features are designed to encourage users to stay on the app, which may be quite addictive.

DAMAGE TO CONFIDENCE

Snapchat's selection of filters and lenses are seen as a great way to enhance your 'selfie game'. Although the filters are often created to promote entertainment and humour, using the 'beatify' filters on photos can set unrealistic expectations and create feelings of inadequacy. Children may strive for admiration and appreciation by sending these 'edited' photos to their friend list. Judging themselves against other users on the app might threaten their confidence or self-worth.

National Online Safety®

Top Tips for Parents

THE RISKS OF SEXTING

It can be slightly awkward talking about this topic with your child, but if it helps them protect themselves, it is worth it. Talk to them about the consequences of sexting and make sure that they're aware of the risks. Ensure your child knows that 'Snaps' can be screenshotted. Teach them that if they post anything potentially embarrassing or harmful (either of themselves or someone else) it can have severe consequences as the message, image or video can be shared further.

REPORTING A STORY, LENS, FILTER, SNAP OR MESSAGE

If your child comes across inappropriate Snapchat content sent directly to them or in another person's story, advise them to report it immediately. This may include an inappropriate lens, filter, message or snap. To report an offensive lens, they should open the app and select the lens they want to report. An info button will appear above the lens. Click this, followed by the flag icon. This will send a report to Snapchat for further investigation. Reports can also be made on the Snapchat support website: support.snapchat.com.

USE 'GHOST MODE'

We highly recommend enabling 'Ghost Mode' on the app so that your child's location will no longer be visible to anyone on the 'Snap Map.' To enable this, go onto the Snap Map and tap the cog in the top-right corner. Here, change the setting to 'Ghost Mode.'

HOW TO DELETE A MESSAGE

Advise your child never to send any negative messages (or images through gallery in the chat on the app) as screenshots can still be taken. You should also advise your child to screenshot any negative comments they receive as the sender can also delete them. To delete a message, simply press and hold the sent message and press delete.

TURN OFF 'QUICK ADD'

'Quick Add' helps friends find each other on the app. This is based on mutual friends or if their number is in their phone book. Explain to your child that this feature can open up their profile to strangers. We highly recommend that your child turns off the 'Quick Add' feature. This can be done in the settings.

RESTRICT STORY VIEWS

Your child can add videos and images to their 'Story' throughout the day which will last for 24 hours. By default, anyone in a user's friends list can see their story. We recommend checking the privacy settings to ensure that this has not been edited. This can simply be done in the apps settings under the 'Who Can View My Story' section. The options to choose from are 'My Friends,' 'Everyone' or 'Custom' - we suggest that it is set to 'My Friends.'

Status of Mind: Social media and young people's mental health | Life in Likes - Children's Commissioners Report | Google Play Store | https://support.snapchat.com/en-US https://netsanity.net/snapchat-parent-review/ | BT.com | Independent.co.uk

Users of this guide do so at their own discretion. No liability is entered into. Current as of date of release: 29/05/19

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform 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 need to know about INSTAGRAM

AGE RESTRICTION 13+ Anyone over the age of 13 can create an account

Instagram is a hugely popular social networking app with over 1 billion users worldwide. The app, which is accessible on iOS and Android devices, allows users to upload images and videos to their feed, create interactive 'stories', exchange private messages or search, explore and follow other accounts they like. Images and videos can be transformed with an array of filters to edit the shot before sharing and anyone with an account can see others' online 'galleries' if their account is not private. To make posts easier to find, users can include searchable hashtags and captions to their uploads. That's why we've created this guide to help parents and carers understand exactly what Instagram is about.

LOCATION

#HASHTAG

HOOKED ON SCROLLING

Many social media platforms, Instagram included, have been designed in a way to keep us engaged on them for as long as possible. Behavioural economist, Nir Eyal, calls this the 'Hook Model' and the Instagram feed is a great example of this. Children and adults may find themselves scrolling to try and get a 'dopamine release'. Scrolling may become addictive and it can be difficult to stop until children find that 'something' they are looking for, quickly losing track of time as they get deeper into their Instagram feed.

SLIDING INTO DMS

Direct messages (or DMs) on Instagram allow users to share posts, images, videos, voice messages and calls between each other privately (or in a private group). Even if your child's account is set to private, anybody has the option to message them and send them content. If the person is not on your child's friends list, the message will still be sent to their inbox but the user has to accept their request to see the message.

INFLUENCER CULTURE

Influencers are sometimes paid thousands of pounds to promote a product, service, app and much more on social media. When celebrities or influencers post such an advert, they should add a disclaimer somewhere in the post which states that they have been paid for it. Commonly, this is well-hidden in the hashtags or in the comments of their post, making it unclear that their photo/video is actually an advert. This can be very misleading to young people who may be influenced into buying/wanting something promoted by somebody they admire, creating a false sense of reality and potentially affecting their mental health and wellbeing.

IMPACT ON WELLBEING

In a report by the RSPH, Instagram was ranked the worst for young people's mental health. Using filters on photos on Instagram can set unrealistic expectations and create feelings of inadequacy. Children may strive for more 'likes' by using realistically edited photos. Judging themselves against other users on the app might threaten their confidence or self-worth. In early 2019, Instagram banned images of self-harm and suicide, following the suicide of 14-year-old Molly Russell, who had reportedly been looking at such material on the platform. They since extended the ban to include drawings, cartoons and memes.

LIVE STREAMING TO STRANGERS

REC REC

Live streaming on Instagram allows users to connect with friends and followers in real-time and comment on videos during broadcast. If your child's account is private, only their approved followers can see their story. It's important to note they may have accepted a friend request from someone they don't know, which means they could be live streaming to strangers. Children also risk sharing content they later regret, which could be re-shared online for years to come. Public accounts allow anybody to view, so we suggest your child blocks followers they don't know. In early 2019, data gathered by the NSPCC found that sex offenders were grooming children on Instagram more than on any other online platform.

IN-APP PAYMENTS

Instagram allows payments for products directly through the app. It operates under the same rules as Facebook Payments, which state that if you are under the age of 18, you can only use this feature with the involvement of a parent or guardian.

EXPOSING LOCATION

Public locations can be added to a user's photos/videos and also to their stories. While this may seem like a good idea at the time, it can expose the location of your child. This is particularly more of a risk if it is on their story, as it is real time. A photo which includes landmarks in the area, their school uniform, street name, house and even tagging in the location of the photo uploaded to Instagram can expose the child's location, making it easy to locate them. If their account is public, anyone can access their account and see their location.

HIJACKED HASHTAGS

Hashtags are an integral part of how Instagram works, but they can come with risks. One person may use a seemingly innocent hashtag with one particular thing in mind, and before you know it hundreds of people could be using the same hashtag for something inappropriate or dangerous that your child shouldn't be exposed to.

IGTV

Instagram TV (IGTV) works similar to YouTube. Users can watch videos from favourite accounts on the platform or create their own channel and post their own videos. It's important to note anyone can create an Instagram TV channel and doesn't have to be friends with a person to follow an account and watch their videos. In 2018 Instagram apologised and removed some of its TV content which featured sexually suggestive imagery of children. As the feature may encourage spending more time using the app, it's important to set time limits to avoid children's sleep or education being disturbed.

@MENTION

Top Tips for Parents & Carers

RESTRICT DIRECT MESSAGES

If your child receives a message from somebody they do not know, encourage them not to accept their message request and 'block' this person; this is the only way to stop them messaging your child again. Children can also 'tap and hold' the individual message to report it directly to Instagram as well as reporting the account itself.

LOOK OUT FOR #ADS

In 2019, the UK's Competition and Markets Authority launched an investigation into celebrities who were posting adverts on social media and not declaring that they were paid for. Influencers must clearly state that they have been paid for their posts, for example using a hashtag like #ad or #sponsored. Teach your child to look out for the signs of a paid post/advert and discuss with them that not everything they see from celebrities is their personal choice and opinion.

MANAGE NEGATIVE INTERACTIONS

If your child is receiving unwanted or negative comments, they can block that account so that they can't interact with them. This stops them seeing and commenting on their posts, stories and live broadcasts. In addition, your child can instantly delete unwanted comments from their posts, turn them off completely and control who can tag and mention them in comments, captions or stories, from everyone, only people they follow, or no one at all.

MANAGE DIGITAL WELLBEING

Instagram now has an in-built activity dashboard that allows users to monitor and control how much time they spend on the app. Users can add a 'daily reminder' to set a limit on how much time they want to spend on Instagram, prompting them to consider if its been too long. In addition, once users have caught up with all the previous posts since they last logged on, they'll receive a 'You've completely caught up' message. Both features can help you have a conversation with your child about how much time they are spending on the app and to set healthy time limits.

PROTECT PERSONAL INFORMATION

Your child may unknowingly give away personal information on their profile or in their live streams. Talk to them about what their personal information is and make sure that they do not disclose anything, including their location, to anyone during a livestream, comment, direct message or any other tool for communication on the platform, even to their friends.

USE A PRIVATE ACCOUNT

By default, any image or video your child uploads to Instagram is visible to anyone. A private account means that you have to approve a request if somebody wants to follow you and only people you approve will see your posts and videos. Children should also use a secure password and enable a two-factor authentication to add an extra layer of security to their account.

FILTER INAPPROPRIATE COMMENTS

Instagram has an 'anti-bullying' filter, which hides comments relating to a person's appearance or character, as well as threats to a person's wellbeing or health. The filter will also alert Instagram to repeated problems so that they can take action against the user if necessary. This is an automatic filter, which should always be enabled. Children can also report abusive behaviour or inappropriate/offensive material directly to Instagram from the app. This includes posts, comments and accounts.

TURN OFF SHARING

Even though this feature will not stop people from taking screenshots, it will stop others being able to directly share photos and videos from a story as a message to another user. This feature can be turned off in the settings. We also recommend turning off the feature which automatically shares photos and videos from a story to a Facebook account.

REMOVE PAYMENT METHODS

If you are happy for your child to have a card associated with their Instagram account, we suggest adding a PIN which needs to be entered before making a payment; this will also help prevent unauthorised purchases. This can be added in the payment settings tab.

DON'T FORGET TO BE VIGILANT & TALK TO YOUR CHILD ABOUT THEIR ONLINE ACTIVITIES!

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 of working in the social media arena and is the founder of Kids N Clicks, a web resource helping parents and children thrive in a digital world.

CHAT

POLL

National Online Safety®

#WakeUpWednesday

SOURCES:
https://about.instagram.com/about-us | https://about.instagram.com/community/safety | https://www.bbc.co.uk/news/uk-47410520

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 03.06.2020

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 of many apps 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

UK AND EUROPE 16+ 13+ REST OF THE WORLD

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

WHAT ARE THE RISKS?

SCAMS

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

DISAPPEARING MESSAGES

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

ENABLING FAKE NEWS

WhatsApp has unfortunately been linked to accelerating the spread of dangerous rumours. In India in 2018, some outbreaks of mob violence appear to have been sparked by false allegations being shared on the app. WhatsApp itself took steps to prevent its users circulating hazardous theories and speculation in the early weeks of the Covid-19 pandemic.

POTENTIAL CYBERBULLYING

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

CONTACT FROM STRANGERS

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

LOCATION SHARING

The 'live location' feature lets users share their current whereabouts, allowing friends to see their movements. WhatsApp describes it as a "simple and secure way to let people know where you are." It *is* a useful method for a young person to let loved ones know they're safe – but if they used it in a chat with people they *don't* know, they would be exposing their location to *them*, too.

Advice for Parents & Carers

CREATE A SAFE PROFILE

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

EXPLAIN ABOUT BLOCKING

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

REPORT POTENTIAL SCAMS

Young people shouldn't engage with any message that looks suspicious or too good to be true. When your child receives a message from an unknown number for the first time, they'll be given the option to report it as spam. If the sender claims to be a friend or relative, call that person on their usual number to verify it really is them, or if it's someone trying to trick your child.

LEAVE A GROUP

If your child is in a group chat that is making them feel uncomfortable, or has been added to a group that they don't want to be part of, they can use WhatsApp's group settings to leave. If someone exits a group, the admin can add them back in once; if they leave a second time, it is permanent.

THINK ABOUT LOCATION

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

DELETE ACCIDENTAL MESSAGES

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

CHECK THE FACTS

You can now fact-check WhatsApp messages that have been forwarded at least five times, by double-tapping the magnifying glass icon to the right of the message. From there, your child can launch a Google search and decide for themselves whether the message was true or not.

Meet Our Expert

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

National Online Safety®

#WakeUpWednesday

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: 02.03.2022

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 of many apps 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 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

18 CENSORED

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

LIVE

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

Friends

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

CAUTION

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.

Sources: www.facebook.com/safety/bullying

National Online Safety®

#WakeUpWednesday

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 30.03.2022

YouTube is a video sharing site/application that enables you to upload, view, rate, share and comment on a wide variety of videos. Consisting of a huge resource of information, advice and entertainment, YouTube now has 1.9 billion logged-in monthly users who watch a billion hours of video daily. Most of the content on Google-owned YouTube is uploaded by individuals, but organisations and media companies also offer some of their content via this platform.

AGE RESTRICTION 13+

What parents need to know about YouTube

SPENDING A PREMIUM

YouTube Premium (formerly YouTube Red) is a new paid streaming subscription service in the UK, offering a three-month free trial to tempt viewers into a £12-per-month plan. This includes the ability to download videos, stream videos with the app in the background, gives exclusive access to original content and a separate music streaming service and gaming app.

DANGEROUS 'CHALLENGE' & VIRAL VIDEOS

On YouTube, 'challenge videos' are shared quickly and can be very dangerous. One person may post a video of themselves doing something unusual like eating a hot chilli or jumping in a river and before you know it, the video goes viral and everyone wants to join in and share their videos. The speed in which challenge videos spread across the Internet makes it difficult to keep up with the latest ones.

SHARING VIDEOS

As well as watching videos, many children are keen to share their own videos online, emulating their YouTube heroes, such as Stampy or DanTDM. However, if they post something on YouTube, they may later regret it or feel embarrassed about what they have shared. There is also a risk that they will receive hurtful or negative comments regarding not only their content, but also their appearance. YouTube's comment section is infamous for being one of the most opinionated on the Internet.

IN-APP MESSAGING

When your child is logged into their Google account and browsing the YouTube website, they can share and talk about videos with their friends using the chat bubble. This can be found at the top right of the desktop site or through in-app messaging on their mobile or tablet. When they tap on the 'Friends' icon, they have a list of suggested people from their contacts – which can be any contact they've had on Google or somebody who has sent them an invite link.

AGE-INAPPROPRIATE VIDEOS

As YouTube is the biggest video sharing website in the world, there is content available for all ages, meaning that some content will not be appropriate for your child. If you think that content is unsuitable, there is a flagging feature to submit it for review by YouTube staff, but you will need to be aware that just because video is not appropriate for a younger audience, it may not violate YouTube's policies. YouTube has mechanisms in place to automatically remove explicit and harmful content, yet offensive content may still slip through.

National Online Safety

Top Tips for Parents

TURN ON 'RESTRICTED' MODE

'Restricted Mode' is an optional setting you can use to help screen out potentially mature content you may prefer your child not to see. Restricted Mode works on the browser or device level, so must be turned on for each browser or device your child uses. To do this, follow these steps:

Desktop:
- Go to the bottom of any YouTube page and switch 'Restricted Mode' to 'ON.'
- To make it more difficult for this to be turned off, you will be given the option to lock restricted mode onto your browser.

Mobile:
- Tap the three vertical dots at the top-right on the screen and press, 'Settings.'
- Click on 'Restricted mode filtering.'
- Press 'Restrict.'

Please note that you can't 'lock' restricted mode on a phone in the same way that you can on a desktop. You will need to turn this on each time your child uses it.

CREATE A FAMILY GOOGLE ACCOUNT

By having a shared family Google account, checking the history will enable you to see exactly what your child is watching and sharing on YouTube. To see the history on a computer, on the right hand menu under the library section, click 'History.' On mobiles, the viewing history can be found by clicking on the 'Library' tab.

BLOCKING ACCOUNTS

When using YouTube, there may be instances where your child receives negative comments. If somebody's giving your child a difficult time, here's how to block them and prevent future comments and replies:

- Go to their channel/account by clicking on their name.
- Click on 'About.'
- Tap the dropdown box with an image of a flag on it.
- Press 'Block user.'
- Tap 'Submit.'

MONITOR WHAT YOUR CHILD IS WATCHING/POSTING

The only way to truly know what your child may have been watching is to regularly monitor them. You can do this by checking their viewing history. YouTube videos can also be easily downloaded, so it is important that your child understands the associated dangers of content they are uploading and that it could harm their online reputation in the future. Show them how to set their videos to private or choose a small network of YouTubers to share with. To get started, your child can use YouTube Studio which offers learning modules on creating a YouTube channel, however, you should encourage them not to use their real name.

NEW FEATURES

DIGITAL WELLBEING

YouTube has launched a tool called 'Time Watched' that allows you to see how long has been spent on the platform. Once you have discovered how much time has been spent on the app, there is the option to set a time limit. Once the limit is reached, a reminder will pop up on the screen. You can also disable sounds and vibrations to help resist the urge to check for notifications.

OPT FOR A FAMILY PREMIUM PLAN

A YouTube family Premium plan may be a cost-effective option if you have more than one child. For £17.99 a month, it allows you to share a YouTube paid membership with up to five other family members – aged 13 and older – living in the same household. As the account holder, or family manager, you must create a Google family account.

MANAGING IN-APP MESSAGES

If your child is accessing YouTube via your account, bear in mind that they may be contacted by Google contacts who are complete strangers to them. You can remove someone from the suggested contacts list by pressing and holding the person's name and tapping on the red 'x.'

POPULAR YOUTUBE GAMERS

There are hundreds of YouTube accounts which show other people playing and commenting on games. These are called 'Let's Play' videos. While YouTube can be a great resource for hints, tips and news for games, it is a good idea for parents to keep a close eye on what YouTuber's are posting. Often, the games they are playing will contain strong language and violence. A few examples of popular YouTube gamers for you to have a look at are:

- Stampy
- Yogscast Lewis & Simon
- PewDiePie
- EthanGamer
- Markiplier
- PopularMMOs
- Captainsparklez
- Jacksepticeye
- LtCorbis
- Dan TDM

!#{?!

SOURCES: : https://www.thesun.co.uk/tech/6702517/youtube-porn-videos-roblox-sex-games-watch-online/, https://www.youtube.com/watch?v=x-frgntP96M, https://www.youtube.com/watch?v=L2xuy7hc-hc http://www.dailymail.co.uk/news/article-5126833/Terrifying-truth-child-watches-YouTube.html, https://www.todaysparent.com/family/crazy-youtube-challenges-kids-are-doing/, https://www.youtube.com/watch?v=4yek0Jb0sBg https://tocaboca.com/magazine/common-sense-media-youtube/, http://familytech.com/so-your-kid-wants-to-start-their-own-youtube-channel/, https://www.laptopmag.com/articles/block-someone-youtube https://www.youtube.com/intl/en-GB/yt/about/brand-resources/#logos-icons-colors, https://www.commonsensemedia.org/blog/popular-youtube-gamers-kids-cant-get-enough-ofStamp

© National Online Safety Ltd
This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

AGE RESTRICTION 13+

Twitter is a social networking site where users can post 'tweets' or short messages, photos and videos publicly. They can also share 'tweets' written by others to their followers. Twitter is popular with young people, as it allows them to interact with celebrities, stay up to date with news, trends and current social relevance.

What parents need to know about Twitter

TWITTER TROLLS

A 'troll' is somebody who deliberately posts negative or offensive comments online in a bid to provoke an individual for a reaction. Trolling, can include bullying, harassment, stalking, virtual mobbing and much more; it is very common on Twitter. The motive may be that the 'troll' wishes to promote an opinion or make people laugh, however, the pragmatics of what they post could be much more damaging, posting anything from racial, homophobic to sexist hate. Trolling can lead to devastating consequences for some victims.

INAPPROPRIATE CONTENT

Twitter gives users the opportunity and freedom to post their personal thoughts and opinions, meaning they can pretty much post anything they want despite restrictions on the platform. Swearing and inappropriate language is allowed if it does not violate the rules. If your child sees any inappropriate content, they might feel the need to replicate it at home or amongst their peers. Additionally, there are also a number of unofficial pornographic profiles on the platform that can easily be found and viewed without restrictions.

FAKE PROFILES

Fake Twitter accounts are made to impersonate a person, celebrity or public figure. As the accounts are not endorsed by the person they are pretending to be, they can often be used to scam or take advantage of young people who think that they're the real deal.

FAKE NEWS

The speed in which 'tweets' are shared on Twitter can be unbelievably fast, meaning that fake news can often be circulated across the platform very quickly. Fake news articles and posts can often be harmful and upsetting to young people and those associated with the fake news. In addition to this, it's very easy for people to quickly and unexpectedly retweet a tweet posted by your child, meaning there is no going back.

HIJACKED HASHTAGS

One of the most commonly used aspects of Twitter is the hashtag (#) – these allow users to easily search for specific trends, topics or subjects. However, due to the astronomical number of Twitter users, many hashtags can have 'different' intentions. One person may use a seemingly innocent hashtag, and before you know it, hundreds of people could be using the same hashtag for something inappropriate or dangerous that your child shouldn't be exposed to. This is common with 'trending' tweets, as people know that their tweet will be seen by a greater number of people.

MEMES NORMALISING RACISM, SEXISM AND HOMOPHOBIA

Twitter is a popular platform for sharing internet memes, helping to make concepts or ideas go viral across the internet. However, despite most meme's being innocent and harmless, some often include sexist, racist or homophobic messages. Although they are typically sent as a joke, this type of content is contributing to the normalisation of topics including racism, sexism and homophobia.

PROPAGANDA, EXTREMISM & RADICALISATION

Social media offers a continuous stream of real-time coverage of extremist activity. Twitter is one of the many platforms that is exploited by extremist groups to help promote violence, radicalise and recruit people to support their cause. These groups cleverly target vulnerable victims, often young people, and find a way to manipulate them into supporting their beliefs.

EVERYONE HAS ACCESS

Twitter has over 335 million monthly active users across all age groups. When a user signs up, tweets are public by default, meaning anyone can view and interact with posts instantly. Your child may change their mind about a tweet they have posted but even if they delete it, there's always a chance that someone can screenshot, retweet it or post it onto another platform.

Top Tips for Parents

CHECK ACCOUNT SETTINGS

We strongly advise that you thoroughly check your child's privacy settings. To take away some of the fear of your child's tweets being shared by anyone, you can always make their account protected. This means that anyone who wants to view what yout child has posted, it requires approval from them. In addition to this, you can change the settings so that they cannot receive 'direct' messages from anyone on the platform and that their location is not shared.

BLOCKING & REPORTING

If a particular account is causing your child trouble on Twitter, whether it's cyberbullying or upsetting content, you can simply block and report them. Blocking them will help to prevent them from viewing, messaging or following your child, and vice versa. Reporting an account will alert Twitter to investigate the profile.

MUTING ACCOUNTS

The 'mute' feature allows your child to remove an account's tweets from their timeline without unfollowing or blocking them. This means your child will stop getting notifications about a particular conversation but can still view it in their timeline. This can be useful if they are friends with someone but don't really like what they share. The other user will not know that they have been banned.

TWITTER TROLLS & THE LAW

From 2016, the CPS were able to exercise new laws that could see those who create 'derogatory hashtags' or post "humiliating" photoshopped images jailed. They also announced the launch of a hate crime consultation, issuing a series of public policy statements centred on combating crimes against disabled people, as well as racial, religious, homophobic and transphobic hate crime. It's important your child knows about building a positive online reputation, as well as showing respect for others online and offline.

SENSITIVE CONTENT

By default, if Twitter has found a tweet that 'may contain sensitive content', Twitter will hide the content in the news feed and you will be shown a warning that states the content is sensitive. You then have the option to view it or not. This gives a chance for you to moderate potentially harmful images/videos before your child sees them. Unfortunately, some content may slip through the cracks and will be shown in the news feed. So, if you do see any sensitive content, you can report it. Twitter should then inspect the tweet and decide whether they deem it to be 'sensitive'.

MUTE HASHTAGS & PHRASES

Within the account settings, you have the ability to block certain words, hashtags or phrases from your child's timeline or notifications (e.g. swear words, inappropriate phrases, emojis, etc.)

TURN OFF VIDEO AUTOPLAY

'Autoplay' is a feature that automatically starts playing a new video seconds after another one ends on the platform. To avoid your child going from watching something innocent and harmless to something much more graphic or disturbing, you can turn this feature off in the settings and easily moderate the videos your child watches before they see them.

CONVERSATION & MONITORING

We always promote that you have regular open conversation with your child about their online activity, ensuring that they understand what healthy relationships are, what respect is, and how to be sensitive towards others' feelings. It's also important to monitor what they're doing online, including what they use the platform for, who they are talking to, and if they are viewing/taking part in anything that they shouldn't be. Discuss the dangers of the online world, such as fake news and online bullying - why do people involve themselves in these activities and what your child can do to prevent them.

TWITTER LISTS

Twitter lists allow your child to create other feeds besides the main timeline that only include certain accounts – this is a great way to segment followers based on common topics and interests.

SOURCES: Sources: https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts | https://help.twitter.com/en/safety-and-security/twitter-location-services-for-mobile | https://help.twitter.com/en/managingyour-account/two-factor-authentication | https://help.twitter.com/en/using-twitter/advanced-twitter-muteoptions | https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public | https://help.twitter.com/en/safety-and-security/public-and-protected-tweets | https://www.statista.com/statistics/493795/twitter-most-retweeted-posts/ | Smallbiztrends.com: 'What is Hashtag Hijacking?': https://smallbiztrends.com/2013/08/what-is-hashtag-hijacking-2.html
Christiededman.com: '5 things you should know about hashtags and your kids': http://christiededman.com/5-things-you-should-know-about-hashtags-your-kids/

National Online Safety

A whole school community approach to online safety

www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061

Reddit is a rather unique site that blends the idea of a social network with news, discussion forums and various other media. The site is broken down into a huge number of categories covering every topic imaginable. Each category is treated as a community and users can submit content for others to see and comment on. This can take the form of links to existing online content or user-generated text and image-based submissions. Submitted content can not only be commented on by others, but also rated using the upvote/downvote system.

AGE RESTRICTION 13+

What parents need to know about REDDIT

SUB-REDDITS

Each community (known as a sub-reddit) has its own set of moderators and its own set of rules, opening up the opportunity for your child to see inappropriate content or something they may find upsetting. Almost every subreddit is user-run, with practically no involvement from reddit employees. Anyone can submit content to a sub-reddit and it's not filtered.

REDDIT GOLD AND GIFTS

Reddit Gold is a premium membership scheme that gives 'extra features to improve the reddit experience,' such as no adverts, custom themes and avatars, and the ability to create Reddit 'secret societies.' Payment costs $3.99 a month (around £3), or $29.99 a year (£23). Users can reward each other for content they post by giving Reddit Gold, a process dubbed 'gilding.' Reddit Gifts is a giant online gift exchange for sending a gift to a randomly assigned user. Reddit recommends that you spend around $20 on a gift, so there is a concern that your child could rack up expenses if unmonitored.

ADULT AND NSFW CONTENT

While there are moderators in place for sub-reddits, they are not necessarily going to ensure that the sort of content you wouldn't want your child to see is banned. Reddit is concerned with free speech and light-touch moderation, so even the most open-minded of people may find deeply offensive content. Reddit generally provides a lot of leeway in the type of content which is acceptable. Some members choose vulgar usernames, while some communities have controversial or rude titles. Some content or communities are marked with 'NSFW' (Not Safe For Work) which means they may contain nudity, pornography, or profanity; it is easy for users to claim to be aged 18 and over to view this content.

REDDIT LINGO

Children and teenagers often manage to mask what they are talking about by wrapping it up in language their parents do not understand. While Reddit is certainly not used just by children and teenagers, like any online community there are words, phrases and abbreviations that may seem impenetrable to start with, such as TL;DR: Too Long; Didn't Read and ITT: In this thread.

CONTENT BIAS AND FAKE NEWS

Subreddits are particularly prone to bias - to the extent that some of them could be seen as propaganda. Reddit has been mentioned as one of the platforms used to promote Russian propaganda, for example. Other news stories can be completely false and not based on any evidence at all – known as fake news - these are written and posted online deliberately to create an impact. Both are nearly impossible to avoid.

TROLLS AND STRANGERS

Globally, millions of people of all ages use the Reddit platform to discuss any topic imaginable from just about every possible viewpoint. Although people can find users who have similar interests, some will choose to abuse the platform. Talking with strangers can lead to trolling and abuse, or your child encountering unsavoury subjects. Reddit users can also send each other private messages, so there is a danger of your child receiving inappropriate or unwanted communication.

National Online Safety

Top Tips for Parents

TURN SAFE BROWSING MODE ON AND ADULT CONTENT OFF

Some sub-reddits are marked as 'adult-only' and in order to access them users must be (or at least say they are) 18 or over. Within your child's user profile, it is possible to indicate that they are not 18 and this will block access to some sub-reddits, but certainly not everything you might consider to be unsuitable. Firstly, to protect them from unsuitable content, check that they have used their correct age when signing up. Secondly, turn off 'adult content' which will disable adult and NSFW (not safe for work) content from showing in the feed and search results. If you are happy to leave 'adult content' turned on, we highly recommend turning on 'safe browsing mode;' this blurs thumbnails and media preview for anything labelled NSFW (not safe for work).

REPORTING CONTENT

To a certain extent it can be useful to learn to just walk away from conversations that take a turn for the worse, but this is not always possible. Learn how to use the blocking feature and teach your child how to use it if someone becomes a problem. Beneath all content and comments that have been submitted by other users, there is an option to report it. Advise your child to report any form of abuse or harassment that they encounter on the platform. It is a good way to alert moderators to the user and hopefully, action will be taken against them.

SPOT FAKE NEWS

Encourage your child to read around topics and not to take something at face value. Just because something is said by someone on Reddit, in no way does this mean that it is true. Remember that the links people post and the comments they leave will cover the full range of political views, intelligence levels and opinions.

LEARN THE LINGO

It is impossible to provide a guide to all the vocabulary and language used on Reddit - it is something that is constantly evolving. There are some words and abbreviations that have become common internet parlance (such as NSFW). If you want to check anything which your child has accessed (which can be seen in the 'Recently viewed links' panel on the front page of the site), be prepared to do a little searching if you encounter things you are unable to make sense of. There's probably a sub-reddit all about acronyms!

BLOCKING STRANGERS

Short of blocking access to Reddit completely, or blocking individual sub-reddits, it's difficult to police your child's use of the site without physically monitoring what they are doing. It is important to let your child know that there are unpleasant people out there and they need to take care about sharing personal information. Should someone start to be a harassment, you can control who can send you private messages and add users to a blocked list by simply clicking on the 'Block User' button.

SOURCES: https://www.reddit.com/r/announcements/comments/827zqc/in_response_to_recent_reports_about_the_integrity/, https://www.reddit.com, https://www.reddit.com/gold/about

© National Online Safety Ltd
This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform 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 need to know about NETFLIX

18+ The account holder must be 18 or older.

Launched in 1997, Netflix is now one of the world's leading online streaming services, providing users with unlimited access to a huge selection of TV shows and films. It's available on any internet-connected device that supports the Netflix app, from smart TVs and games consoles to tablets and smartphones, and is becoming increasingly popular with a younger audience. This is unsurprising given consumer attitudes are changing more towards video-on-demand (VoD) services. That's why we've created this guide to help parents and carers understand exactly what Netflix is about.

Inappropriate content

Netflix hosts and produces content for all ages. It has a wide variety of films and TV programmes for young children, teens and adults and its extensive catalogue can provide hours of entertainment. Children can search for almost anything but if they share the same account as an adult, it can also open them up to viewing material that is adult themed or inappropriate. Netflix doesn't check who's watching so children could access films or tv shows that contain violence, nudity or foul language.

Risk of hacking

With millions of users in over 190 countries, Netflix is often targeted by hackers and phishing scams which try to illicit usernames and passwords to gain access to accounts. If successful, hackers can steal payment details or try to sell your data on the dark web, providing others with the opportunity to profit. Given Netflix doesn't provide 2-factor authentication, its important to ensure your login details remain secure.

Binge-watching

With the ability to access Netflix on almost any device, it can be easy to fall into 'binge-watching' TV series, with users finding it difficult to turn it off without knowing what happens next. The autoplay function also means that the next episode usually plays within seconds of the last ending and the Netflix algorithms mean that recommended programmes are very often similar to those you've just watched. This can easily lead to spending hours in front of the TV through the day or staying up through the night, potentially affecting sleep, mood and the ability to concentrate the next day.

Screen addiction

In addition to binge-watching, the fact that Netflix is available on almost any device with an internet connection means that parents may find it difficult to prize children away from a screen. With a huge collection of children's TV programmes and the latest film titles, children could start watching on the TV, continue on the tablet and finish on their games console. Increased screen time means that they may spend less time learning, playing outside, find it difficult to sleep or communicate less with family and friends.

Netflix party

Netflix Party is a free extension on Google Chrome that gives users the ability to watch a film or TV show online simultaneously with friends or family in different locations. It also provides the ability to chat to each other during the stream. Users can create a party and send a link to people they want to invite however the link can be copied and distributed further, meaning children could potentially be open to a group chat with people they don't know. It should be noted that Netflix Party isn't an official Netflix product and needs to be downloaded separately to the app.

National Online Safety®

#WakeUpWednesday

Safety tips for parents & carers

Create a Netflix Kids experience profile

One of the biggest advantages of Netflix is the ability to control what content your children can watch. Setting up a Netflix Kids experience profile means that children only have access to TV shows and movies which have been carefully selected for kids. The look and feel of the app is simpler and children can't access any account settings.

Set maturity ratings & block content

If your child is a little older, parents can create a separate profile to their own and set a maturity rating that means children will see only TV shows and movies that fit that rating. The three categories of rating for the UK are kids (all, U, PG), teens (12, Guidance, Teen) and adult (15, 18, mature, adult). You can also block specific TV shows and movies from individual profiles which means they don't show up in the browse or search results.

Have an open & honest conversation

Parents can review the TV shows and films that have been watched on each profile under their account. If your child seems upset or shocked by something they have seen or if you are concerned about anything they've viewed, try to talk to them about it and have an open and honest conversation to help understand any concerns.

Switch off autoplay

Netflix has two autoplay features that can be switched on and off across different accounts and takes effect across all devices. Parents can disable the ability for consecutive episodes to play automatically and for previews to play when browsing. Both can help to limit the amount of time children spend on the app.

Lock your profile

It's important to keep your own account secure so that children can't freely switch between profiles and potentially access more adult-themed content or change access levels. Parents can set-up a Profile Lock PIN which means only they can access their own Netflix account.

Set screen time limits

Although switching off autoplay will help to stem programmes playing continuously, children can just as easily choose to play the next episode themselves. Whilst Netflix has no options to help limit viewing time, many devices now allow parents to set screen time restrictions, so you can switch off the app automatically when you think they've had enough.

Create a strong password & always log out.

Given that Netflix doesn't use 2-factor authentication, the need for a unique username and strong password is even more important. Try to use a different password to ones you've used before and use a mixture of numbers, letters (uppercase and lowercase) and symbols, with a minimum of 8 characters. Always log out when not using your account so that if your device is lost or stolen, your account remains inaccessible.

Meet our expert

Pete Badh is a writer with over 10+ years in research and analysis. Working within a specialist area for West Yorkshire Police, Pete has contributed work which has been pivotal in successfully winning high profile cases in court as well as writing as a subject matter expert for industry handbooks.

SOURCES: https://www.netflix.com | https://help.netflix.com/en/node/264 | https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 22.02.2020

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 of many apps 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 DISCORD

AGE RATING 13+

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

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

WHAT ARE THE RISKS?

CYBERBULLYING

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

DIFFICULT TO MODERATE

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

INAPPROPRIATE CONTENT

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

ACCESSIBLE TO PREDATORS

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

CRIMINAL ACTIVITY

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

Advice for Parents & Carers

REVIEW SAFETY SETTINGS

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

EXPLAIN AGE FILTERING

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

SCREEN OUT EXPLICIT CONTENT

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

MONITOR ONLINE ACTIVITY

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

DISCUSS GOOD ONLINE BEHAVIOUR

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

HAVE CANDID CONVERSATIONS

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

Meet Our Expert

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

National Online Safety®

#WakeUpWednesday

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://ktalk.com/discord-deleted-thousands-of-violent-extremist-and-crim-1545622614

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

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

FaceApp, as the name suggests, is an app by Wireless Lab which uses uploaded images of someone's face and allows them to add a variety of interesting filters making themselves look older, younger, appear with different hair colour and so on. The app uses either the camera on your phone to take a selfie, or lets you use a picture from somewhere like Facebook or Instagram to apply these filters. While this all sounds like innocent fun, there have been some valid concerns raised about the terms and conditions, and what the company is doing with all these selfies and pictures.

AGE RESTRICTION

13+

If under 18, supervision of a parent or legal guardian required.

What parents need to know about FACEAPP

WHY IS IT SO POPULAR?

The app went viral in the middle of July 2019 with the #faceappchallenge, where users download Faceapp, take a picture of their face adding the old age filter, and then share the image of themselves online with friends. It can be fun to see what you might look like when you're more well travelled, and the results are pretty convincing (much to the amusement of older family members!).

HOW DOES IT WORK?

The app scans the uploaded face, and uses a neural network (basically a huge database of sample faces) to show what it thinks you'll look like when you're old; adding wrinkles, grey hairs, yellowed teeth etc. Anybody can upload an image they have access to, even those of children, without any kind of consent being needed. As explained in the lengthy terms and conditions of the app, these images are saved by Wireless Lab and can be used however they see fit, at any time in the future.

IS IT SAFE?

This is the contentious question. Wireless Lab, the Russian company behind the FaceApp app, are particularly vague with their descriptions of what they can potentially do with a person's details, to the point where a lot of people are worried about their images being used for nefarious purposes like cyber crime or political campaigns. In reality, the app is no more or less safe than any other, but that doesn't mean you shouldn't be vigilant of what you or your child is agreeing to online.

LEVEL OF ACCESS?

Buried in the legal jargon and technical mumbo jumbo, FaceApp has a worryingly large amount of access to your or your child's device. As well as storing any pictures you upload to the app, it also has access to your internet history, and basic information like your name and location. Naturally this sounds scary because it has been highlighted so publicly, but this is the normal kind of access and information apps take from us nowadays. If you are at all concerned it's worth leafing through those lengthy Terms Of Service before making a decision on if you're happy for your child to use an app.

SHOULD I BE WORRIED?

While your details COULD be used in the wrong way, the company has publicly stated they have no desire to do so and a number of independent probes into the app seem to suggest everything is being stored correctly and safely. That's not to say it will always be this way, so it's worth bearing in mind that this could change further down the line.

FACIAL RECOGNITION SOFTWARE

An app that takes an image of a face and uses it to commit online crimes or say things pretending to be somebody else might sound like the plot of a hollywood thriller, but with today's technology it can be a very real fear. Facial recognition software is now so advanced, a fake picture or video of a face can be produced without your knowledge or permission, potentially by a company you thought was safe. Now it must be stressed that this is extremely unlikely to happen, especially as this advanced technology is still being worked out, so you shouldn't be too worried about it - but always be aware of the permissions you're giving to unknown parties.

National Online Safety

#WakeUpWednesday

Safety Tips For Parents

CHECK DOWNLOADS

It may seem obvious to keep an eye on what is downloaded on a device, but it can be very easy to miss out on new fads and viral hits. Most app stores let you see what's currently trending, alongside descriptions of what an app is. Talking to your child about what current trends they're enjoying will help you keep an eye on what's popular. You also get to see what you might look like in the future, which could be a blessing or a curse!

BE REALISTIC ABOUT YOUR DATA

When it comes to online security, the phrase 'better the devil you know' is particularly apt. While companies like Facebook and Google are by no means virtuous in their collection of our data, we do at least know (for the most part) a lot about how it's being handled. Luckily, we know Wireless Lab are treating our information correctly for now, but apps you don't know or trust, may not. It's always worth reading up on an app and making sure it's the real deal before downloading it.

BE AWARE OF COPYCAT APPS

When something like FaceApp goes viral, many copycat apps can pop up on the store piggybacking off the success of the original. These apps can contain viruses that are often far more malicious and dangerous to you and your child than the terms in the 'safe' version of the app. Make sure you're aware of which is the original before making any downloads.

KNOW IF YOU CAN SPEND MONEY ON AN APP

Like most things these days, there is a way to spend money on FaceApp. You can purchase a 'pro' version which unlocks additional filters either through your phone's app store, or on the app itself. This subscription ranges from 1 month for £3.99, 12 months for £19.99 or lifetime access for £38.49. It's very easy to make this purchase without too much thought so do make sure you know about any additional costs of an app your child is using.

ALWAYS READ THE TERMS AND CONDITIONS

Many of us don't have the time or energy to read through pages and pages of legal speak, and that's normal, but leafing through the fineprint can unearth a lot of grizzly permissions you didn't know you were giving. Often, at times they are unavoidable, but knowing what you're signing up for and if there's anything you can do about it could help you make more informed decisions on the types of content you expose your child to.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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://www.techradar.com/uk/news/is-faceapp-safe-a-deeper-look-at-the-viral-hit, https://www.tomsguide.com/news/faceapp-photos-privacy-worries, https://fortune.com/2019/07/17/faceapp-safe-privacy-russian-old-face-app/ https://www.unilad.co.uk/technology/faceapp-could-be-sharing-all-your-photos-without-you-knowing/, https://www.faceapp.com/terms

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 23.07.2019

Did you know?
IT IS ILLEGAL TO TAKE, MAKE OR SHARE AN INDECENT IMAGE OR VIDEO OF A CHILD UNDER THE AGE OF 18 – EVEN IF IT IS CONSENSUAL

Sexting occurs predominantly on, but is not exclusive to these apps...

Snapchat | Tinder | WhatsApp | Kik

Sexting involves sending and receiving explicit messages, images or videos of a sexual nature. This content is usually uploaded on a mobile device, which can then be uploaded onto social networking sites and shared further. They can be sent to or from a friend, boyfriend, girlfriend, or someone your child has met online. Sexting is often described as the new flirting for children – but it is illegal for anyone under the age of 18, with police forces in England and Wales recording 6,238 underage "sexting" offences in 2016-17, a rate of 17 a day.

What parents need to know about SEXTING

BREAKING THE LAW

Sexting is illegal if you share, make, take or distribute an indecent image or video of a child under the age of 18. It is an offence under the Protection of Children Act (1978), the Criminal Justice Act (1988), and under Section 67 of the Serious Crime Act (2015). Sexting or 'youth produced sexual imagery' between children is still illegal, even if they are in a relationship and any images are shared consensually.

CHILDREN THINK IT'S HARMLESS

Many young people see sexting as 'banter' or a joke, an easy way to show someone they like and trust them, or just a cool thing to do. But they may not realise the consequences of sharing personal information and how it can be potentially harmful to them in the future.

REGRETTING THEIR ACTIONS

Although some children are willingly exchanging images, many may regret sharing the messages, images and videos after they have sent or uploaded them. Once it's out there, there's no going back, and your child may feel ashamed, vulnerable, worried or anxious about imagery resurfacing later, especially if a relationship or friendship has broken down. 'Sexting' was the most viewed information and advice topic on the Childline website in 2017, showing the need for people to get help.

BULLYING, COERCION & BLACKMAIL

Your child may feel pressured into sexting, so they don't come across as boring, or think it's a way to show someone they care for them. They may feel under pressure to give in to repeated requests or feel obliged to share sexual messages and imagery. Sexting can also expose young adults to the risk of being exploited by paedophiles or sexual predators, who then use images to extort additional photos, sexual favours, and sometimes money from victims.

SHARING

Once a photo or video is out there, there's no way of knowing how many people have saved it, tagged it or shared it. Children like to show off to their peers and suddenly, an image has gone beyond its intended recipient, to classmates, friends, and even strangers. Once an image or video has been shared online, there's nothing to stop it being archived and repeatedly shared.

Top Tips for Parents

TALK TO YOUR CHILD

Encourage open dialogue about appropriate information to share with others both online and offline, discuss the word 'sexting' and ensure that they know what it is and what it involves. Show that you understand that sexting can reflect natural adolescent curiosity about nudity, bodies and exploring their sexuality, but explain why it's important to think twice before sharing something. Show that you are approachable and understanding.

DISCUSS THE LEGALITIES

Children and young people may not realise that what they are doing is illegal. Ensure that your child understands that when they are aged under 18, it is against the law for anyone to take or have a sexual photo of them – even if it's a selfie, and even when the activity is consensual.

EXPLAIN THE REPERCUSSIONS

Let your children know that once they have sent a message, they are no longer in control of it, and the messages, images and videos that they may intend to share with one individual may end up where the whole world can have access to them. Even if they completely trust someone, other people using their phone might accidentally see it. And, later in life, it may affect their online reputation, especially if universities, employers or future partners access the imagery.

HOW TO REMOVE IMAGES

If an image has already been shared, either your child or yourself should speak to the person that the image was shared with and ask them to delete it. You can also use the report button on a website where the image was posted. Speak to your child's school, as they may be able to confiscate phones if they know that they have sexual imagery stored. If you believe the child was forced into sending the message, report this to the police. You or your child can also report the content to CEOP with one of their child protection advisors (Child Exploitation and Online Protection Command).

BLOCKING AND STOPPING SEXTING

Show your child how to use the block button on their devices and favourite apps to stop people sending them unwanted messages. You can also set up parental controls with your internet service provider or on your child's phone to stop them from accessing harmful content.

HAS YOUR CHILD RECEIVED A SEXUAL IMAGE?

Firstly, reassure your child that they have done the right thing by speaking to you about the incident. Ask them if they requested the image or if they received it unwillingly. If the image has been sent to your child by an adult and you are concerned about sexual exploitation or grooming, contact CEOP immediately.

SOURCES: NSPCC (2015) Review Under Pressure: What's Affected Children in April 2013 - March 2014. [online] nspcc.org.uk/globalassets/documents/annual-reports/childline-review-under-pressure.pdf. Last accessed on 25/07/18; theconversation.com/one-in-seven-teens-are-sexting-says-new-research-92170; learning.nspcc.org.uk/research-resources/childline-annual-review; bbc.co.uk/news/uk-41880500

National Online Safety

A whole school community approach to online safety

www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061

'Fortnite - Battle Royale', is a free to play section of the game 'Fortnite'. The game sees 100 players dropped on to an island from a 'battle bus' where they have to compete until one survivor remains. The last remaining player on the island wins the game. Players have to find items hidden around the island, such as weapons, to help them survive longer in the game. To make the game harder, there is an added twist called 'the storm', which reduces the size of the island from the start of gameplay, making the players closer together in proximity. The game is available on PC, PlayStation 4, Xbox One, Mac and iOS.

What parents need to know about FORTNITE: BATTLE ROYALE

MICROTRANSACTIONS

New featured items are released daily and are only available to purchase within 24 hours of their release. These are cosmetic items, called 'skins', 'gliders' and 'emotes', which change the look of the characters but do not improve the game play. Once purchased, the player has full use of these in the future. The designs are made admirable for players to purchase and even celebrities are endorsing them. Also available to purchase in the game is a 'Battle Pass'. When a new 'Battle Pass' is released, users can play a series of challenges to receive more rewards (cosmetics) by progressing through different tiers. Whatever rewards they achieve can then be used in the game.

IT CAN BE ADDICTIVE

Games can last around 20 minutes but this varies with each game. Children may feel angry if they lose the game and continue to play until they achieve the result they want. The competitive nature of the game may make it difficult for children to stop playing halfway through as it could affect their position in the game.

IT CAN BE PLAYED ON THE GO

The game was released on mobile in April 2018 meaning it can be played without a games console at home. Some schools have reported that the game is distracting their students whilst in the classroom. As the game is available outside of the home, parents may not be aware of how long their child is on the game.

HACKER ATTACKS

News site Forbes said it had seen "dozens" of reports online by people who said their accounts had been compromised by hackers. Hackers gained access to users accounts in the game and spent hundreds of pounds in fraudulent charges.

TALKING TO STRANGERS DURING SQUAD MODE

Interacting with other players in the game is part of the fun as players can communicate with their friends and other players in the game. Players will benefit from wearing headphones in the game to hear footsteps from other players trying to compromise their game. Wearing headphones makes it difficult for parents to hear what exactly is being said and children may be exposed to inappropriate language. Fortnite includes really good reporting features for players either cheating or misbehaving, and work towards having one of the best online gaming communities.

'FREE' TO PLAY

The game IS free to play. However, if playing on Xbox, you will need an Xbox gold subscription to play the game which is chargable.

NO PROOF OF AGE REQUIRED

Signing up to the game is relatively simple. Users have the option to log in with their Facebook or Google accounts or their email address. When signing up with an email address, there is no proof of age required. If your child is under the age of 12, it is important to check if your child has the game downloaded.

SOCIAL MEDIA SCAMS

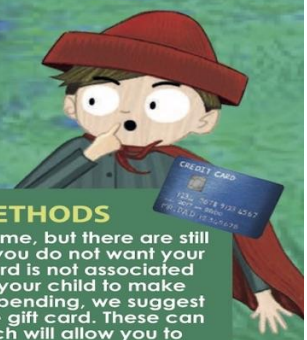
There are many accounts on Facebook and Twitter which claim to give away free money (known as 'V bucks') for games which will be transferred to their Xbox Live or PSN cards. Any giveaway promotion from Fortnite will be in game. It is important to check the authenticity of these accounts before giving away personal information in order to claim 'v bucks'. The websites or accounts may ask you to share your account name and password in order to claim the money; if these offers seem too good to be true, they usually are.

WEAPONS AND VIOLENCE

PEGI has given the game a rating of 12+. Even though the game includes violence and weapons such as crossbows, grenade launchers, rifles, pistols, shotguns and more, PEGI say "more graphic and realistic looking violence towards fantasy characters is allowed. Any violence towards human characters must look unrealistic unless it consists of only minor or trivial injury such as a slap", making the game 'suitable' for children aged 12 and over.

National Online Safety

Top Tips for Parents



#1 LIMIT GAME TIME

Parents can use parental controls on Xbox and PC to limit the time your child is playing games on the devices. Be aware that the game is available on iOS and will soon be available on all mobiles. With this in mind, it is worth having a conversation with your child to discuss and agree how long you would like them to spend on games. Even though the games last around 20 minutes, it may be hard to take them away from a game mid play. It may be worth using a limit of the amount of matches they play rather than a time limit.

#2 RESTRICT PAYMENT METHODS

'Fortnite: Battle Royale' is a free to play game, but there are still options to make additional purchases. If you do not want your child to make payments, ensure your card is not associated with their account. If you are happy for your child to make payments in the game, but want to limit spending, we suggest using a paysafecard, or a games console gift card. These can be purchased in specific amounts, which will allow you to limit how much your child spends and removes the need for a credit/debit card to be used with their account.

#4 PREVENT THEM TALKING TO STRANGERS

There is an option to turn off the voice chat feature, which means they wouldn't be able to talk to anybody, including their friends. Your child will still be able to use the in-app chat and hear other people's conversations. To turn off voice chat, open the Settings menu in the top right of the main Fortnite page, then click on the cog icon. Open the Audio tab at the top of the screen. From there, you can turn off voice chat.

#3 SHOW THEM HOW TO MAKE A REPORT

If your child believes a player is playing or talking inappropriately, you should advise them to report them. To report a player, you can use the in-game feedback tool located in the Main Menu of the game. Additionally, you can report a player in-game when spectating them.

#5 LOOK OUT FOR VBUCK SCAMS

It is important that your children are aware of the scams that they may come across online in association with the game. Open up conversation with them about scams and how they should never share their username or password with people in order to gain anything for the game.

#6 USE A STRONG PASSWORD

It may seem like a simple tip, but it is important that your child selects a strong password when creating an account, particularly if a credit/debit card is associated with the account. This will help reduce the risk of their account being hacked.

Sources
https://www.microsoft.com/en-gb/store/p/fortnite-deluxe-founders-pack http://www.bbc.co.uk/news/newsbeat-43626075
http://fortnitehelp.epicgames.com/ https://pegi.info/ https://www.forbes.com/sites/erikkain/2018/03/12/
fortnite-accounts-hacked-how-to-protect-yourself-and-what-to-do-if-youve-been-compromised/#140c9e7ca7f9

© National Online Safety Ltd
This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

www.nationalonlinesafety.com

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

FIFA20

You don't need to be the biggest football fan in the world to have heard of FIFA (Federation Internationale de Football Association) - the governing body for football. And, the video game series bearing the organisation's name is one of the most successful ever. The lure of this football series is that official licensing gives your child the opportunity to play games in the role of their favourite players. They can either work through a story mode version of the game or play online in competitions against other players. The game, released annually by Electronic Arts under the EA Sports label, is available for a range of consoles, and there are also mobile versions available for smartphones and tablets.

AGE RESTRICTION

3+

If under 18, supervision of a parent or legal guardian required.

What parents need to know about FIFA 20

CONSTANT SERIES REFRESHES

The big selling point for the FIFA range of games is that it FIFA includes current players; a feature which no other football video game offers. However, this means that a new version of the game is released every year, with updated teams, players and stadia, plus new gameplay features and tweaks. And, with every annual update of the game, there is an expectation that it will be far better than the previous one, so the pressure to upgrade and buy the new version is likely to be immense!

FAKE EMAILS AND SCAMS

Your child may receive an email or see a message on social media or in forums which appear to be a genuine FIFA promotion. While the link may seem like a FIFA login page, it's a phishing scam to capture a login name and password. Scammers may use names that sound legitimate, like 'EA Admin' or 'FIFA Developer'.

JUST ONE MORE GAME

Your child could be playing FIFA games on their computer or console for very long periods of time. That's not to say that computer-based matches are a full 90 minutes long, but a series of 20-minute matches can very quickly fill up a day! The World Health Organisation has classified 'gaming disorder' as a mental health problem - this is when children have trouble controlling their gaming behaviour and let it reign over their lives and daily routine.

IN GAME CHAT

While the FIFA video game is suitable for children of all ages as it does not include any inappropriate content, there is the issue of in-game chat. Your child can play with other people online and chat with them using headsets. As this is largely unregulated, it could mean that your child is exposed to language or conversations that you deem unsuitable.

BUYING ADD-ONS

In-game purchases are to be expected in any modern game and FIFA is no different. FIFA Ultimate Team (commonly called FUT) is a mode in FIFA that lets gamers build teams of players from any league, playing both offline and online to win coins. These can be used to buy better players or packs containing random players. While some purchases can be made using in-game currency, other purchases involve spending with real world money, which could become expensive. There have been reports of parents receiving large credit card bills resulting from in-game purchase made by their children.

FIFA GAMEPLAY

The FIFA series has been criticised for the competitive nature of gameplay leading to aggression in some players. Add to this the chance to converse with other players via in-game chat, and the potential for anger levels is likely to rise... especially if you're losing heavily!

National Online Safety

#WakeUpWednesday

Top Tips For Parents

ABOUT THE SERIES REFRESHES

As a parent, the implications of this really depends on the age of your child and your relationship with them. It may be that playing and sharing games is part of your family life and so this isn't a problem, but just be mindful that being involved with the FIFA franchise is unlikely to be a one-off event - it's the start of a gaming journey that could last for many, many years and involve numerous (potentially expensive) upgrades.

STEER CLEAR OF SCAMMERS

You should teach your children to stay clear of scams. Explain to them that they must be wary of any link which asks them to either verify their username and password or provide other sensitive information; game developers will never send a message asking for login information. Console messages, emails and websites, or social media posts promoting contests for in-game content, such as packs, players, or coins requiring login information are fake.

MONITOR ACTIVITY

The parental controls on consoles can be used to restrict the amount of time spent playing. Physically monitoring how much time your child is spending in FIFA is recommended - just as you might monitor how much time they spend watching TV. Keep an eye out for warning signs, such as a lack of interest in other activities, tiredness or fatigue, neglect of personal hygiene, changes in character or anger issues whe your child is told to stop playing a game.

HAVE THEM REPORT ABUSE

It's unlikely that you'll be able to convince your child to play FIFA without making use of the chat facility - it's something that adds to the experience. However, you should ensure your child is aware of how to silence any abusive players and how to report anyone who becomes problematic.

RESTRICT PURCHASES

To spend real money in FIFA, a credit or debit card must be linked to a gaming account, so ensure that your card is not being used for this! There's also support for PayPal payment, so also check who has access to this type of account. Depending on the platform your child is using to play FIFA, there are different parental controls that can be put in place to restrict spending should you allow them to link a card to their account. There is also a payment option called Paysafecard, which allows you to make payments online without the use of a bank account or credit card. As you can top up balances, this makes it easy to control spending.

ENCOURAGE BREAKS

Monitoring in-game chat may be difficult as you're likely to only be able to hear one side of a conversation. However, noticing how your child is reacting may be a reasonable indicator of the general mood. Dealing with both the frustrations of a game as well as troublesome people can serve as useful life lessons, but as a parent, you know your child better than anyone else. If you notice your child is getting too upset or angry, that's the time to intervene and try to encourage them to take a break from the game.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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

http://press.ea.com/products/p1532/ea-sports-fifa-18, https://help.ea.com/en-gb/help/fifa/be-safe-with-fut-coins-and-fifa-points/

https://www.telegraph.co.uk/men/relationships/fatherhood/10886939/My-son-spent-hundreds-of-pounds-on-in-app-purchases-without-me-knowing.html

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 06.11.2019

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

There's a very good chance you've heard of Minecraft. The block building phenomenon is, arguably, the most beloved video game of all time which has managed to maintain its popularity since its first release back in 2011. Nine years later, it still has a huge userbase of 112 million people playing the game every month. Accessible to those 7+, Minecraft can be a gateway into a world of learning and exploration which encourages players to use their imagination to build three-dimensional worlds with virtual building blocks. While Minecraft is considered relatively safe generally speaking, there are some safety precautions parents may want to consider before allowing their children loose on the game.

AGE RESTRICTION 7+ If under 16, supervision of a parent or legal guardian required.

What parents need to know about MINECRAFT

OPEN TO HACKING

Hackers can be a real problem in any online game, including Minecraft. Some individuals can access other people's games to disrupt their play time, or even worse, access private details about players such as their names, email addresses, dates of birth and so on. It would be incredibly rare and unfortunate to encounter a player like this, but it does happen and must be taken as a serious risk.

RISK OF GRIEFING

Griefing is when someone purposely upsets another player during the game. This can be done by ruining somebody's creation or generally doing something to spoil someone's gameplay and can essentially amount to a form of cyberbullying. In open servers, or even private ones among friends, it can be difficult to keep track of who's saying what, and an innocent comment in one person's eyes could be seen as bullying by somebody else. Stealing supplies, destroying things that take hours to build and harassing innocent players can all be commonplace if care isn't taken.

CONTACT WITH STRANGERS

Most players aged 7 and over will be able to play the game comfortably and, whilst creating an account does ask you to input your date of birth for confirmation, there's no way to check if the information is correct nor to check someone's real identity. This could mean that children younger than 7 could access the game. However, what is more concerning is that adults pretending to be children could theoretically be using false information to access the game and be interacting with your child.

ADDICTIVE NATURE

Minecraft can be an incredibly exciting game but it can also be very addictive. Too much time on the game could impact on your child's behaviour, causing them to become irritable or angry when being asked to stop playing. This might suggest it might be time to enforce some time away from the game. Addictive behaviour can be compounded at a young age and encouraging gaming in moderation is always recommended.

'SCARY' CHARACTERS FOR YOUNGER GAMERS

For the most part, Minecraft is not a scary game. Despite this, there are certain characters in the game that younger children in particular may find frightening. Creepers, zombies and various other 'baddies' can be commonplace in some parts of the game and young minds may find it difficult to disassociate them from real life once they switch off the game.

National Online Safety #WakeUpWednesday

Safety Tips For Parents

BLOCK STRANGERS AND UNWANTED CONTACT

Despite the fact that private messages can no longer be sent in the game, strangers may still attempt to interact with your child. From the pause menu, players can block chat and friend requests from others in the game. This causes any profanities, email addresses and phone numbers to become automatically blocked, meaning it's harder for people you don't know to potentially contact your child.

LEARN FROM YOUTUBERS / TWITCH STREAMERS

There are a lot of Minecraft focused YouTubers and Twitch Streamers that offer a huge variety of fun, engaging content. Many of them focus on making videos specifically for younger audiences, which don't include bad language or anything scary. If you're unsure about the game, check out some of the biggest streamers and more importantly, ask who your children like. This will help you to understand what the game is about and also make sure that your children are watching age-appropriate content online.

PLAY IN CREATIVE OR PEACEFUL MODES

Playing the game on Creative or Peaceful mode ensures that the experience is strictly safe. Peaceful mode allows children to explore with friends without having the survival element of normal Minecraft, while Creative mode allows imaginations to run wild with unlimited resources, encouraging creation of vast, personalised worlds. There really are no limits as to what can be accomplished and getting involved yourself can make it a great way to bond with your child and give you a long-term project to complete with them.

MONITOR GAME TIME

Being able to play on a wide variety of platforms can be beneficial however it can also make it more difficult to put the game down. Play time should be monitored and it's always a good idea to talk to your child if you feel they are spending too much time on the game or showing signs of addictive behaviour.

CREATE A PRIVATE SERVER

The best way to avoid unwanted strangers or griefers in a server is to simply create your own. Private servers do exactly what they say on the tin by offering a safe, secure place for children to play and create with their friends, free from outside interference. They (and you) control who is allowed in the server and what kind of things they can do in it, making it the closest thing Minecraft offers to parental controls.

LEARN TO PLAY YOURSELF

Minecraft is an incredibly easy game to pick up and play. Furthermore, it doesn't require an expensive console or computer, with versions available for smartphones and tablets. Learning to play yourself and playing alongside your child is the best way to understand the game and will help to put your mind at ease in respect of what your child is viewing and who they may be interacting with.

CREATE SERVER WHITELISTS

Usernames you know to be safe, like your child's friends or relatives, can have their accounts whitelisted as safe. Essentially, this means that server moderators can create a community made up of people they know to be friendly and children will only be playing alongside people both they and you know, reducing any risk of contact with strangers or experiencing griefing.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 15.01.2020

ROBLOX
Powering Imagination

According to the Roblox website, 'Roblox is the world's largest interactive social platform for play'. For those of you not so familiar with the game, it is a multi-player online gaming platform which allows children to play and create a variety of games in a 3D world. Roblox is free to play and available on all modern smartphones, tablets, desktops, Xbox One, Oculus Rift, and HTC Vive.

What parents need to know about ROBLOX

ROBLOX STUDIO

The Roblox Studio allows users to create their own games and 'worlds' for others to play on the platform. As the games are user generated, it gives users the freedom to potentially include things you do not want your child to be exposed to, for example, weapons, violence and even pornographic content. There are no age restrictions on the games created in the Roblox Studio and Roblox can only rely on people reporting negative/violent content in order to remove the games from the platform.

CHATTING AND FRIEND REQUESTS

Whilst the games in Roblox are aimed at 8 to 18-year-olds, there are currently no age restrictions for signing up. This means both adults and young people can play and communicate with each other and send friend requests through the platform. Once a friend request is accepted, this means that they can communicate with each other outside of gameplay.

ROBUX ONLINE PAYMENTS

When a user creates a game, they earn something called 'Robux', which works as a currency within the platform, allowing the purchase of upgrades and memberships. If the created game is of good quality and attracts multiple players and in-game adverts, children have the potential to earn a lot of 'Robux'. Once a user has earned a certain amount of Robux, they can convert this to real cash and withdraw it to a PayPal account. To withdraw money, users need to be over 13, have a PayPal account and have paid for the Roblox premium subscription.

NOS National Online Safety

Top Tips for Parents

UNLIST SOCIAL MEDIA ACCOUNTS

Make sure your child's social media accounts are not listed in the settings/account info. If they are, advise them to make them private or remove them in their account. This will ensure nobody can find and contact them on their social media platforms outside of Roblox.

CHECK SHARED INFORMATION

In the account settings, check that your child is not giving away any personal information in their bio/profile. For example, their full name, phone number or snapchat name. If you see that they have, explain why this is potentially dangerous and remove immediately.

2 STEP VERIFICATION

Roblox has a great 2-step verification security feature which we recommend you enable to add an extra layer of security to your child's account.

HAVE A CHAT ABOUT 'GRIEFING'

Griefing is when someone purposely upsets another player in a game. This can be done by setting traps, damaging or stealing something from another player, intentionally killing them and just generally doing something in the game to spoil gameplay for them. Essentially, 'Griefing' is a form of cyberbullying and can be extremely frustrating and upsetting for players.

IS YOUR CHILD UNDER 13?

Unfortunately, there are hundreds of YouTube videos showing children how to change their age settings on Roblox, so firstly, you should talk to your child to set up some rules/an agreement. There are additional safety features for children under 13, for example having their posts and chats filtered for inappropriate content and behaviour, so It is worth checking that your child has set up their account with the correct age. You can find this in their account settings.

DISABLE IN-GAME CHAT

Roblox is great for children to play together and chat to each other. However, if you wanted to completely turn off in-game chat for your child (meaning they could not contact anyone including their friends) you can do so by following these steps: When logged in, go to the Account Settings page by clicking on the gear icon at the top right corner of the page, then click Settings. Next, click on the Privacy tab and under 'Who can chat with me in game?' select 'No one' and this will disable in-game chat.'

RESTRICT PAYMENT METHODS

Roblox is a free to play game, but there are still options to make additional in-game purchases. If you do not want your child to make payments, ensure your card is not associated with their account. If you are happy for your child to make payments in the game, but want to limit spending, we suggest using a games console gift card. These can be purchased in specific amounts, which will allow you to limit how much your child spends and removes the need for a credit/debit card to be used with their account.

Source: corp.roblox.com and press kit - All images shown belong to Roblox ©2018 Roblox Corporation. Roblox, the Roblox logo, Robux, Bloxy, and Powering Imagination are among our registered and unregistered trademarks in the U.S. and other countries.

© National Online Safety Ltd
This is not a definitive guide. Please always check with the app's support information to see if your security and privacy concerns are addressed.

www.nationalonlinesafety.com

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

Microsoft Teams, or simply 'Teams', is a platform that allows for collaborative working, either as students or as professionals, using communication capabilities through audio, video and instant messaging. The software is available both online through a web browser and to download from microsoft.com. Users can have 1:1 online meetings or set up live events to host up to 10,000 people. Groups can be set up to include only relevant users and almost all file-types can be uploaded and shared, from PDFs and Word documents to audio and video files.

AGE RESTRICTION 13+

What parents need to know about MICROSOFT TEAMS

DISCLOSING PERSONAL DETAILS

Like any messaging service or social network, children can be targeted by others to share their private or personal information ranging from their phone number, birthday and home address to their social media accounts or even their personal login details and passwords. Oversharing their private information can lead to any manner of risks including online fraud, bullying or even grooming activity.

CYBERBULLYING

The risk of cyberbullying can be increased online when using chat facilities. Microsoft Teams provides the ability for users to chat to each other via its instant messaging service, both as part of a group or privately. Children could find themselves the target of negative or hurtful comments directed from other users who might find it easier to say things they maybe otherwise wouldn't in person.

INAPPROPRIATE CHAT

The chance to have private conversations in Teams can also mean that children feel as though they can share messages and communication between each other that are hidden away from others. Whilst children are most likely to use Teams in a school setting, the ability to chat privately may provide an opportunity to be less formal which could lead to sharing inappropriate messages, files or content which is unsuitable in a school environment.

HACKING RISK

Teams, like any software application, may be a target for hackers to illicit personal data. A 'man-in-the-middle attack' could occur, whereby the attacker reroutes communication between two users through the attacker's computer without the knowledge of the other users. This means that online communications could possibly be intercepted and be read or listened to, exposing both parties to the possibility of identity fraud or other criminal behaviour.

VIRUS INFECTION

Viruses and other harmful programs are among the risks of using online platforms like Microsoft Teams. Wherever you can share files or links, there is a risk that the content could be malicious. This could lead to slow computer performance, deletion of data, the theft of private or personal information and even hackers taking control of your PC.

LIVE STREAMING RISKS

Microsoft Teams, like other video-conferencing software platforms, facilitates live streaming. That means it inevitably carries some of the associated risks. These are likely to be minimal within a controlled environment (for instance in a classroom setting / remote learning). However, live streaming means that content isn't always moderated and children may inadvertently view or hear inappropriate, unsuitable or offensive material that they otherwise wouldn't.

National Online Safety
#WakeUpWednesday

Safety Tips for Parents & Carers

BLOCK USERS

If your child is receiving inappropriate messages or finds themselves being harassed or abused on Teams, they can block these contacts from the privacy control in the settings menu. To add an extra layer of protection, you can also block contacts whom hide their ID to protect children from communicating with people they don't know.

PROTECT PERSONAL INFO

It's a good idea to talk to your child about the importance of keeping their personal information private and secure. Children should only give out the minimum information they need to when creating an account and understand that if other people request their personal details from them, they should avoid providing it and report any concerns to a trusted adult.

ENABLE BACKGROUND BLUR

To help protect your privacy during a video call or live stream, it may be a good idea to blur the background or even add a background effect. This can easily be done by clicking 'Background effects' before joining a meeting after which you'll have the option to blur your background, replace your background with one of the images provided or upload and use an image of your own.

UPDATE COMPUTER SECURITY

It's important to ensure you perform regular computer and software updates, as these patches often improve security flaws and minimise your vulnerability to cyberattacks. Having your own computer security or anti-malware software is another level of defence in minimising the chances of an attack from viruses, malware and other harmful programs. Ensure this is updated everyday so that it is able to protect you against the very latest threats.

TALK ABOUT RISKS

As a parent, talking to your child and making them aware of the risks of working and communicating online can help them to be more digitally resilient. Perhaps outline a set of agreed do's and don'ts and try to ensure young people know what to do if they are made to feel uncomfortable or experience any negative behaviour or activity.

AVOID VIDEO/AUDIO

It's always a good idea to turn off your audio during live group calls when not in use. This can easily be done by muting the mic and will avoid others hearing anything personal in the background at home or at school. Similarly, if possible, try to encourage children to avoid using video call to help guard against any privacy concerns and limit the risks of viewing anything inappropriate or unsettling.

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.

SOURCES:
https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/group-chat-software
https://www.microsoft.com
https://www.thinkuknow.co.uk

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 10.06.2020

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

Founded in 2011, Zoom is one the world's leading video conferencing software providers. It has a number of features, including video and audio conferencing, real-time messaging, screen-sharing and the ability to upload, share and search for content. Users can start their own meetings or they can join meetings set up by others. The app is available to use across PCs, laptops, tablets and mobiles phones and is free to download on both the app store and on Android.

What parents need to know about ZOOM

ZOOM BOMBING

'Zoom bombing' is the term which has been coined to describe unauthorised people joining zoom meetings uninvited and broadcasting pornographic or inappropriate videos. An attacker can hijack a meeting if they know the meeting ID and it isn't reinforced with a password. Not taking preventative measures or implementing privacy controls could open up the risk of children witnessing sexual or inappropriate content with very little notice.

RISK OF PHISHING

The rise in popularity of Zoom has led to a rise in hacking operations and phishing campaigns. This is when participants are encouraged to click on links to join what they believe to be legitimate Zoom meetings via email, but which are in fact fraudulent. These scams aim to obtain sensitive information such as user login details, passwords and/or credit card information.

PRIVACY CONCERNS

Depending on how the app has been set-up, Zoom can offer very little privacy. In many cases, the meeting hosts can see detailed information about each participant including their full name, phone numbers and maybe even location data. Furthermore, depending on where the camera has been set up or where your child's computer is positioned, private or personal information could be stolen depending on what can be seen in the background.

LIVE RECORDINGS

One of the features of Zoom is the ability to record live meetings. By default, only the host of the meeting can usually record live sessions however other meeting members can also record if the host gives them access. Recordings can be stored on devices or on the cloud and can be downloaded and shared with no restrictions. This means that videos, audio clips and transcripts of recordings involving your children could be widely shared on the internet or between users without your authorisation or consent.

PRIVATE ZOOM MEETINGS

Zoom has a facility to set up breakout rooms, which enables a private meeting within the main Zoom session. The host can choose to split the participants of the original meeting into separate sessions. This gives children the ability to speak privately away from the main group to other users however chats aren't always monitored by the host and if the meeting has been made public, children could be more vulnerable to experiencing negative comments.

'LIVE STREAMING' RISKS

At its very core, Zoom facilitates live streaming. That means it inevitably carries some of the associated risks that live streaming brings. These are likely to be minimal within a controlled environment (for instance when used in a classroom setting for remote learning). However, live streaming means that content isn't always moderated and children who use the app unsupervised or with limited security settings, may be more at risk of exposure to viewing inappropriate material. Other risks can include downloading malicious links, sharing personal information or even potential grooming.

Safety Tips For Parents

REPORT INAPPROPRIATE CONTENT

Remind your child that if they do see something that makes them feel uncomfortable or upset then they need to talk about it and report it. Parents can report unwanted activity, harassment, and cyberattacks to Zoom directly. To help your child, you could try setting up a checklist before they go online, with an agreed set of rules and what they should do if they see something inappropriate.

USER PRIVATE MEETING IDS & PASSWORDS

It is always better to set up a meeting with a random ID number generated by Zoom than by using a personal number. This means it is harder to guess and less likely to be hacked. It's important to never share meeting IDs with anybody you don't know and always set-up a password function to allow other people to sign-in. This should already be a default setting that is applied on Zoom.

PROTECT YOUR PERSONAL DATA

It's important to discuss with your child that they should not share personal information on Zoom. This includes passwords, their address, phone number, etc. Create your child's account under a false name or pseudonym and always set a custom background to help hide details in your home. Zoom allows you to turn on virtual backgrounds and select your own image to appear behind you.

BEWARE OF PHISHING EMAILS

Every time you or your child gets a Zoom link, it's good practice to ensure it has come from the official platform and is not fraudulent. Signs of a phishing email include an unrecognisable email address, an unofficial domain name or a slightly distorted logo. The email itself might also be poorly written or contain suspicious attachments.

TURN OFF UNNECESSARY FEATURES

If your child is using Zoom, there are a number of features that you can turn off to make the experience safer for them. For instance, disabling the ability to transfer files or engaging in private chats can help to limit the risk of receiving any malicious attachments or receiving any inappropriate messages. In addition, you can turn off the camera if it is not needed or mute the microphone when not in use.

USE THE 'VIRTUAL WAITING ROOM FEATURE

The waiting room feature on Zoom means that anybody who wants to join a meeting or live session cannot automatically join and must 'wait' for the host to screen them before entering. This is now a default function and adds another layer of security to reduce the likelihood of zoom bombing.

KEEP YOUR VERSION UPDATED

It's important to ensure you are using the latest version of Zoom available and always update it if you get a prompt. These updates are usually to fix security holes and without the update you will be more vulnerable to an attack. Check the official website to see what the latest version is and compare it to your own.

HOST IMPLEMENTED PRIVACY CONTROLS

If your child is part of a larger group meeting, then it's important to make sure that the host is abiding by Zoom's Terms of Service. This includes the fact that they have gained everybody's permission for the session to be recorded. The host should also have set screen sharing to 'host only' and disabled 'file transfer' to help keep the live stream secure.

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://zoom.us/privacy | https://zoom.us/ | https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf
https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 08.04.2020

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

oculus quest

The Oculus Quest is the latest virtual reality experience on the market. Taking advantage of ever-evolving technology in the industry, the Quest can offer unparalleled levels of realism that really need to be experienced to be believed. From colourful cartoon worlds to photorealistic monsters, it can be the perfect tool to experience everything this, and countless other, worlds have to offer. As with any other gaming hardware, it's important to know how to use it safely and ensure children are aware of any potential risks. That's why we've created this guide to help parents and carers understand exactly what the Oculus Quest is all about.

AGE RESTRICTION 13+

If under 18, supervision of a parent or legal guardian required.

What parents need to know about OCULUS QUEST

ONLINE VIRTUAL CHAT

Much like on other gaming platforms, chat rooms and multiplayer games can be a lot of fun, but also a place where others may look to approach and groom young people, often masquerading as somebody younger to appear more trustworthy. There are a whole host of chat rooms available in VR and each will have their own safety features and rules, so be aware of which your child might be using, and never leave them unsupervised while talking to strangers.

PHYSICAL INJURIES

Wearing a virtual blindfold can inhibit your knowledge of the real world around you. Young children playing could easily forget where trip hazards or pieces of furniture are and stumble into them causing some quite nasty injuries. It's recommended that you have at least 6 square feet of clear space before playing a VR game. Oculus devices come with an option to program a virtual barrier in line with your real-life play area.

MOTION SICKNESS & SEIZURES

The health and safety warning that comes with the Oculus Quest estimates that roughly 1 in 4,000 people are susceptible to having a seizure while playing VR. This is the same number as those playing video games, watching TV or any activity that involves a screen and bright lights. If a child has photosensitive epilepsy it might be best to avoid VR altogether, or at the very least consult a doctor before playing.

INTENSITY RISK

Aside from the age rating of the Oculus Quest headset, VR is a super-heightened realism and can be an intense experience. Frightening, violent or anxiety provoking content may cause your body to react as if it were real and it's important to choose content appropriately. Whilst there are no medical studies linking VR specifically to increased rates of depression and anxiety, if you're noticing changes in your child's behaviour, it could be time to think about limiting exposure.

OVERUSE CONCERNS

Given that virtual reality is a relatively new concept, there has been little research into its long-term effects on children. For the most part, headsets will be completely safe however manufacturers themselves advise against prolonged use as it could negatively impact hand-eye coordination, balance, and multi-tasking ability. With this in mind, it's important to note that most VR headsets carry a recommended age of 13+, regardless of the games you plan on playing.

National Online Safety®

#WakeUpWednesday

Safety tips for parents

TAKE REGULAR BREAKS

It's estimated that somewhere between 40-70 percent of people who use VR will feel motion sickness during their experience. In simple terms, this happens when the eyes and the brain disagree with what is happening to the body. The resulting feeling of nausea can last all day, and be particularly distressing for younger children. If at any point motion sickness starts to set in, turn off the headset, get some fresh air, a drink of water and sit down away from any screens!

TRY IT YOURSELF

As with anything, the best way to understand VR is to try it yourself. There are various experiences to undertake that range from entertaining to educational. If you're confident guiding your young ones through the amazing possibilities virtual reality has to offer, it can be an amazing activity to do together.

ENSURE CORRECT SETUP

A poor-fitting VR headset can lead to an uncomfortable experience and lead to an impaired sense of motion and balance. Taking a few extra minutes to make sure the Quest's mounting is secure and comfortable can make a huge difference and ensure children play safely. Adjusting the image focus to be sharp and clear is also very important to reduce eye strain while playing.

USE GAME COMFORT RATINGS

VR experiences can be incredibly realistic. With that in mind, Oculus has a comfort guide which appears next to games on the online store. The guide ranges from comfortable to intense (and unrated) to help give an idea of what kind of situations might be present in any given title. As always though, use your own judgement about what is suitable for your children.

LIMIT EXPOSURE TIME

It is recommended that players take a 10-15 minute break from VR every 30 minutes or so to keep eyes from becoming strained or minds disoriented. This is the case with any video game, but especially important in VR because it's a whole-body experience. Children will always be able to pause a game or finish the round before putting the headset to one side and enjoying life in the real world once again.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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://support.oculus.com/quest/
https://www.insidescience.org/news/cybersickness-why-people-experience-motion-sickness-during-virtual-reality

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 08.07.2020

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

VR - or Virtual Reality to you and me - is the practice of creating computer generated images or sometimes even entire worlds for a user to experience as if they were there. Whereas traditionally we'd use a television screen to view these images and games, technology now allows us to simply put on a headset with much smaller screens inside and become fully immersed in these new worlds. While virtual reality is perfectly safe on the whole (although sometimes you might feel like you're in real, physical danger) there are some things to look out for if you plan on giving it a try.

AGE RECOMMENDATION 13+

What parents need to know about

VIRTUAL REALITY

IS VR SAFE FOR CHILDREN?

Broadly speaking, VR is safe. The technology being used is so young however, that we don't fully understand the long term repercussions of using it just yet, if indeed there are any. Because of this, it can be hard to know how much screen time is too much and what games and experiences are going to be okay for children. Thankfully, there are a whole host of interesting and educational applications that we can be pretty confident using. Things like 3D art games and sports/activity apps can be a unique way to experience endeavours that might be otherwise difficult to pursue.

IS MY HOME VR READY?

The first big question to ask is 'do I have enough space?' Most modern VR headsets will require an area of clear floor space to work so you can walk around a little, move your arms and generally explore. How much space you need is a matter of which headset you have and what you're using it for, but generally speaking the absolute minimum you'll want is about 5 or 6 feet cubed which will allow you to turn and move your arms without venturing too far. Naturally you'll want to also make sure there are no pieces of furniture or precious ornaments within swinging distance as stubbed toes and broken vases are no joke!

THE EQUIPMENT YOU NEED

Many VR kits come with a dizzying selection of bells and whistles which can seem quite daunting at first, but all you strictly need is a headset with a screen and a headband. While the minimalists will be able to enjoy a virtual tour of an aquarium or a safari, many games will need you to incorporate controllers or headphones to really get the most out of it. Thankfully, the majority of VR kits include a headset, any wires you'll need to connect it to your home entertainment device, some basic headphones and special controllers. Some may also come with sensors which you'll be required to place at the corners of play area so it knows how much room you have.

OPTIONS AVAILABLE

The headset you buy will depend on what you're looking to use VR for and your price range. Many headsets are age restricted. For example the Oculus Rift and Samsung VR carry an age gate of 13+, the PlayStation VR is for 12 and over, while HTC Vive specifies that it is not for young children at all. Nintendo LABO is for 6 and up, while the low-tech Google Cardboard doesn't carry an age warning at all. Each of them offer their own unique perks and pitfalls so if you're unsure, a cheap headset that can be used with your phone and some downloaded apps is a good place to start.

ONLINE FEATURES

As with normal consoles, some VR games will have a multiplayer portion. Anybody with a headset and the game will be able to play with each other online, and not all games will carry a robust safety system. If you know your child is using a game that can be played online, be sure to check on its safety features.

IS VIRTUAL REALITY THE SAME AS AUGMENTED REALITY?

AR

VR

Not to be confused with virtual reality, augmented reality - or AR - superimposes a computer generated image into the real world and doesn't require a headset. Games and apps like Pokemon GO or the upcoming Minecraft Earth use this technology to make it seem like something fictional is on the screen in front of you. This is usually achieved on a mobile phone screen, but the technology already exists to use things like tables, mirrors and other household objects.

National Online Safety

#WakeUpWednesday

Top Tips For Parents

VR CHAT GAMES

Some games involve a sort of online, VR chat room where you can talk to other people all around the world, with the most popular among these being VRChat. VRChat uses a fairly good Trust and Safety System, that goes some way to protecting against nuisance users or profiles. Do make sure you read up on how these systems work before letting a child use them, especially if it's another chat game you're not familiar with.

MEDICAL CONDITIONS

VR can be a rather disorienting experience at first and some people may begin to feel nauseous or uncomfortable after an extended period of play as their brain struggles to understand its new digital surroundings. This is known as 'Virtual Reality Sickness.' Although quite common, it's important to stop once these feelings arise. If you, a family member or friend have any underlying health issues too, it may be wise to consider if VR is the right option as it could put unknown stresses and strains on the body.

ENFORCE BREAKS

As mentioned, VR can be a disorienting experience that does take some getting used to. Committing to regular breaks (every 15-30 minutes or so) will hopefully stop VR sickness from setting in.

DON'T BE AFRAID TO TRY IT YOURSELF

The beautiful thing about virtual reality is that it's not just used for gaming. You can discover untold treasures from across the world or try your hand at painting a masterpiece, all from the comfort of your own home. Having a good understanding of how everything works will enable you to enjoy it alongside your child and while new technology can be daunting, it can also be incredible to experience. By and large, it's much easier to get to grips with VR games than regular ones because you're the controller!

ALWAYS SUPERVISE INTERACTION TIMES

VR is not like a normal games console as essentially you're running around blindfold from the real, physical world. Tripping, breaking and falling into things can all occur if you're not careful. Make sure you're keeping a watchful eye on what's happening without getting in the way yourself. Nothing says 'I got too close to somebody playing VR' like an unintentional bump on the head.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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.

https://home.bt.com/tech-gadgets/computing/gaming/virtual-reality-gaming-virtual-reality-how-much-does-it-cost-and-is-it-safe-11364193115313,
https://www.scientificamerican.com/article/are-virtual-reality-headsets-safe-for-children/, https://www.techradar.com/uk/how-to/when-is-it-safe-to-buy-kids-a-vr-headset

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 31.07.2019

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

There's a good chance you already know what the PlayStation 4 (PS4) is. Sony's video game console is often touted as being one of the best-selling of all time, with over 100 million units shifted worldwide. With over seven years of polishing and fine-tuning under its belt, you'd expect the console to be one of the safest around. While this is overwhelmingly true, there are still things parents should be on the lookout for whether they're children are starting it up for the first time or they're already experienced users.

AGE RESTRICTION
GAME SPECIFIC PEGI RATING - See Individual Title Packaging

What parents need to know about PLAYSTATION 4

Playstation Store

SAFETY CONCERNS

PlayStation users are able to add each other as friends by simply inputting another players' username and sending them a friend request. If accepted, they can chat openly from the console's dashboard, including voice chatting in a private party. If players know each other, this can be a great way to talk privately while in games, without having to interact directly with others. But, similarly, if a stranger adds a child and is accepted as a friend, they have direct access to them.

ACCESS TO PERSONAL INFORMATION

The PlayStation Network (or PSN) is essentially used to house all the other PlayStation services (like PlayStation Plus and PlayStation Store) under one roof. Accounts are free and come in two forms; master accounts and sub accounts, with master accounts having access to the parental controls on a console. If a user's ID and account password were compromised (if a child was tricked into revealing it or if a hacker obtained the details otherwise) then it could provide access to personal information or banking details.

ONLINE BULLYING

Sometimes in an online game, players will be able to freely chat with each other. While these interactions will mostly be positive and about having fun in a game, some people will take this opportunity to use offensive or abusive language or may just want to aggravate other players. In some cases, it may amount to harassment, trolling or cases of online bullying.

ADULT CONTENT IN GAMES

The PlayStation offers a huge variety of different games, all with different age ratings. From shooting games to driving, sports, educational titles and everything in between, they all need special attention when considering a purchase, as some can contain adult content or explicit language with isn't always suitable for young children. The best way to know what a game involves is to check out its PEGI rating which will be on the game box, or on the website page before you buy. Remember that these ratings serve as a guide, and the ultimate choice lies with parents to know what is acceptable and appropriate for their children.

PEGI 18+

SCREEN ADDICTION

The PS4 can provide hours of entertainment. As well as being an avenue to play games, it provides the ability to browse the internet, watch live TV or stream video services such as Netflix, Amazon or YouTube. Such is the variety, that it can be easy to switch between modes and rack up time in front of the screen. Some children may also find it difficult to control the amount of time they play games, potentially leading to gaming disorder.

National Online Safety #WakeUpWednesday

Safety Tips for Parents & Carers

CREATE 'CHILD FAMILY MEMBER' ACCOUNTS

The PS4 allows parents to set up different accounts for different family members, including children. This will allow you to control different aspects of your child's PS4 experience including the ability to set age restrictions on gameplay, limit play time sessions, disabling chat messaging and the ability to access the internet.

DISCUSS PSN RISKS WITH YOUR CHILD

It's always a good idea to discuss with your child how to stay safe on the PlayStation Network and how to respond if people they don't know contact them. Advise your child to report anybody who upsets them or makes them feel uncomfortable and to never share personal or private details or images with anyone online. You can also block other users if they are abusive or your child feels threatened by their behaviour.

SET MONTHLY SPENDING LIMITS

It's a good idea to set a limit on how much can be spent on things like new games, or for skins or card packs in games like Fortnite and FIFA. This can be done using your master family account and then selecting your child's account. Go to Applications/Devices/Network Features from where you should be able to select Monthly Spending Limit and adjust it as you see fit.

IMPLEMENT PRIVACY CONTROLS

Sometimes it's easier to block potential risks at the source when playing online. Through Network Features, you can select whether a child's sub account can communicate with others while on the PSN or whether they can view content created by other players. This means disabling the ability for your child to communicate via chat or messages or displaying and entering comments for friend requests and game invitations. It also means you can block videos, images and text created by other users from view.

SET AGE RATING LEVELS FOR GAMES, DVDS AND BLU-RAYS

As well as controlling what age rating level of a game your child can play, you can also set appropriate controls for DVDs and Blu-Rays. To set this up, simply go through the Family Management setting and then Applications/Devices/Network Features and select the type of content you would like to restrict.

12+ 18+

LIMIT PLAY TIME

Play time can also be managed through the PlayStation's parental controls. On the family manager accounts, go to Settings, Parental Controls, Family Management and select the child account you'd like to limit play time for. From here, set a Time Zone, then configure the Play Time Settings to your preference.

15 30

KEEP ACCOUNTS SECURE

To stop children from changing parental controls and adjusting their own limits and restrictions, you can create a system restriction passcode to disable guest login and set up a log-in passcode so that only you can access your account. To protect against hackers, you can activate 2-step verification (2SV) which will alert you of any new logins. You can also set up a password at 'checkout' in the PlayStation Store so that there is an additional layer of security if anybody attempts to make any unauthorised purchases.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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://www.playstation.com/en-gb/get-help/help-library/my-account/parental-controls/ps4-parental-controls/ | https://www.playstation.com/en-gb/get-help/help-library/my-account/parental-controls/online-safety/ https://www.playstation.com/en-gb/get-help/playstation-safety/ | https://www.playstation.com/en-gb/get-help/help-library/my-account/parental-controls/play-time-settings/

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 13.05.2020

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform 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 ...

PLAYSTATION 5

The PlayStation 5 is the next-generation video game console from Sony. It offers improved graphics, sound and much quicker loading times. It also has a new controller with motion- and force-feedback features for a more immersive experience. Parents should note that there are two different versions available that support discs or digital downloads.

Safely setting up your Playstation 5

PlayStation 5 Blu-ray

PlayStation 5 Blu-ray is the larger of the two consoles, although not by a lot. It enables you to play games on disc or by digital download. Although all new games are available digitally, the disc drive is still useful to watch movies from discs as well as play most existing PlayStation 4 games you own. It also enables you to purchase second-hand games on a disc, which is often much cheaper.

PlayStation 5 Digital

PlayStation 5 Digital is slightly smaller as it doesn't contain a Blu-ray drive. This means the console is cheaper but can only run games you download via an internet connection. Unlike the Xbox Series X and the cheaper Series S, the digital-only PlayStation 5 is just as powerful as its more expensive disc-and-download counterpart.

Family Settings

Both PlayStation 5 models offer important family controls that should be set up before your family starts using the system. Although this can take a little time, it ensures that children have their own accounts and sets limits on spending, interactions and age ratings. If done correctly, children cannot circumvent these controls that require the parent's password to alter.

Downloading the PlayStation App

The PlayStation 5 uses the same PlayStation app as the PlayStation 4. This is a super-easy way to tweak the user settings for your family without having to log on to the console. It's also a good way to keep track of what different people are enjoying on the system. The app can also be used as an easier way to log-on by scanning the QR code.

Setting Limits on Play Time

You can specify how long, and at which times of day, the console can be used to play without needing a password. Talk to your children and agree how long is appropriate, then set this on their profile, so it's something they understand and accept. You can set different time limits on each of the users on the system.

Creating Guest Account Password

An important step during the PlayStation 5 set-up is specifying the default settings for guest accounts as well as a passcode for your own account. This ensures that all users need to access the system with their own account and related limits and settings.

Managing Spending

You can set a limit on spending via Parental Controls. This means that any additional purchase requires your password. Another alternative is not to put credit card details into your account and instead add credit as they need it using the book token-like cards in-store or online. A nice feature on the PlayStation is setting an amount of pocket money to spend on games each month.

Managing Online Interactions

Another important area of the Parental Controls is specifying how and who your child can interact with online. Modern consoles enable players to share text, voice, images and video with each other. You can set whether they can do this, and also apply a password before they can add new friends.

Setting Age Ratings

You can set a limit that stops any older-rated games being played without a password being entered. This is not only a good way to ensure children are playing appropriate content but is a good chance to talk about the games they are playing.

Game Subscriptions

In addition to buying individual games digitally or in-store, you can also subscribe to services that offer access to hundreds of games for a monthly fee. PlayStation Plus is needed to play games online with other people and offers a set of games you can immediately download for the new system. PlayStation Now enables you to stream (and download) a wider set of games.

Types of Accounts

Set up Parent Accounts

Setting up a parents' account is important so you can manage the console for your family. After plugging your console in, connect to the internet and wait for updates to finish. Once updated, create a parent user account with an email address you regularly check and password specified.

Set up Child Accounts

Setting up child accounts are important to be able to limit play time, spending and apply age ratings automatically. Separate accounts for each child user can be set up. It's a good idea to specify a password for the guest account so children cannot access this also.

Meet our expert

Andy Robertson is a freelance family technology expert who often works for the BBC. He runs the Family Gamer TV YouTube channel and contributes to a range of national media on the topic of video games and family.

National Online Safety®

#WakeUpWednesday

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 25.11.2020

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform 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...

XBOX SERIES X|S

The Xbox Series X and Series S are the next-generation video game consoles from Microsoft. They offer improved graphics, sounds and much quicker loading times. Parents should note that the two versions available are quite different.

Safely Setting up Your Xbox Series X / S

Xbox Series X

Xbox Series X is a larger device, with a disc drive, twice as much storage and higher performance chips. It can play the new Xbox games at the highest resolution and with the best visuals. It enables you to run games from disc or digitally.

Xbox Series S

Xbox Series S is a smaller, disc-less version of the console which plays all the new games but with reduced visuals or possibly frame-rates. Because it doesn't support discs you can't play old games from discs and must purchase new games digitally. It also has smaller storage, offering 500GB which is about half that of the Xbox Series X.

Apply Family Settings

Both Xbox models offer important family controls that should be set-up before your family starts using the system. Although this can take a little time, it ensures that children have their own accounts and sets limits on spending, interactions and age ratings. If done correctly, children cannot circumvent these controls that require the parent's password to alter.

Setting Age-Ratings

You can set a limit that stops any older rated games being played without a password being entered. This is not only a good way to ensure children are playing appropriate content but is a good chance to talk about the games they are playing.

Managing Spending

You can set a limit on spending via the family settings. This means that any additional purchase requires your password. Another alternative is not to put credit card details into your account and instead add credit as they need it using the book-token-like cards in-store or online.

Managing Online Interactions

Another important area of the Family Settings is specifying how and who your child can interact with online. Modern consoles enable players to share text, voice, images and video with each other. You can set whether they can do this, and also apply a password before they can add new friends.

Setting Limits on Play-Time

You can specify the time of day and how long the console can be used to play without needing a password. Talk to you children and agree how long is appropriate, then set this together so it's something they understand and accept. On the Xbox Series X|S you can also limit time on a particular game, which is a good way to encourage children to play a wide range of experiences.

Creating Guest Account Password

An important step on the Xbox Series X|S set-up is specifying a passcode for your own account and a password to access the Guest account. This ensures that all users need to access the system with their own account and related limits and settings.

Game Subscriptions

In addition to buying individual games digitally or in-store, you can also subscribe to services that offer access to 100's of games for a monthly fee. Xbox Game Pass is often bundled with the Xbox Gold subscription you need for playing online. Most of the bigger Xbox games are provided as part of the service, as well as a wide range of independent games that often offer educational and wellbeing based experiences.

Types of Accounts

Set-Up Parent Accounts

Setting up a parents account is important so you can manage the console for your family. After downloading the Xbox app to aid set-up, connect to the internet and while the console updates, use the app to start specifying settings. Once updated, create a parent user account with an email address you regularly check and password specified.

Set-Up Child Accounts

Setting up child accounts are important to be able to limit play-time, spending and apply age ratings automatically. Separate accounts for each child user can be set-up. It's a good idea to specify a password for the guest account so children cannot access this also. You can also download the Xbox Family Settings app to help you adjust these settings in the future without having to access the console directly.

Meet our expert

Freelance family technology expert for the BBC. Andy runs the Family Gamer TV YouTube channel and contributes to a range of national media on the topic of video-games and family.

National Online Safety®

#WakeUpWednesday

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 11.11.2020

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

NINTENDO SWITCH

The Switch is a hybrid console released by popular video game company Nintendo in 2017. It's classed as a hybrid because it's designed to be played both at home on a television, like traditional consoles (think a PlayStation or an Xbox) or out and about like a portable console, such as a GameBoy. It uses two detachable and wireless 'Joy-Con' controllers on either side of the console's screen, which can be used by one or two players. The Switch can be played on the internet with the purchase of Nintendo Switch Online, in the living room together or on the go during long journeys, but bear in mind it needs to be charged just like anything else!

AGE RECOMMENDATION 6+

What parents need to know about NINTENDO SWITCH

NINTENDO SWITCH ONLINE

Nintendo Switch Online is a paid service that allows the console to be played (you guessed it) online, by linking to other Switch consoles around the world. It can be purchased through the Nintendo eShop for a single account on the device, or with a family membership plan which covers 2 accounts. The purchase options come in three tiers; 1 month, 3 months and 12 months but be aware these auto-renew unless you specify otherwise.

ONLINE DANGERS

While online, your children will be able to play with and chat to people on compatible games, which will mostly be good-natured fun, but could potentially expose them to vulgar language, indecent images or worse. There are options to limit this though, which are detailed below. It's worth remembering that many games can be played offline, so while it's not essential to get Nintendo Switch Online, it is certainly something to consider.

NINTENDO eSHOP

The Nintendo eShop is where games can be purchased over the internet and downloaded directly onto the device. If you choose to enter your bank details (or PayPal account) onto the Switch, you can save them for easy access later on. Do note however that these can be viewed by anybody with access to the console, unless you specify otherwise. A child might accidentally purchase a game or item from the shop if these details are left improperly protected, which could leave you with a nasty surprise.

NINTENDO'S VIDEO GAME SELECTION

Nintendo as a company offers some of the most entertaining and safe video games on the market. Games featuring characters like Super Mario, Donkey Kong and Yoshi are always a safe bet for a child-friendly experience. It's always prudent to check each game before you buy it (especially if the game hasn't been made by Nintendo) but as a rule of thumb, anything official containing well-known names like these will be great for your children, giving you peace of mind while they enjoy them.

PORTABLE GAMING

Being able to take the Switch anywhere is a huge bonus when travelling. What's more is that almost every game can be enjoyed without the need to 'dock' the console with a television. Battery life on the Switch varies depending on what it's being used for but typically it will last around 3 or 4 hours before needing to be recharged. When the time comes, any USB-C charger will be able to do the job, but it's best and quickest to return it to the dock, which requires a normal plug socket.

National Online Safety
#WakeUpWednesday

Top Tips For Parents

PARENTAL CONTROLS

Nintendo released a free downloadable app that can be used in tandem with the Switch called Nintendo Switch Parental Controls. Once you've got the app on your mobile device, it's a simple process to pair your two devices, giving you a suite of options to help make sure your child is having fun in a safe and structured environment curated by you.

ONLINE RESTRICTIONS

Another major inclusion in the app is the ability to block your child from seeing anything to do with age restricted games. There's also an extremely helpful feature that restricts access to games that have free communication features between strangers on the internet. This includes things like private messages and unsolicited images. Should you be concerned that strangers might be using the games to talk to your child, a simple press of a button will disallow any access they might have.

PLAY WITH YOUR CHILD

One of the wonderful things about the Switch is that there are an abundance of great games you and your child can enjoy together, and even with the whole family. Nintendo has a long history of making and supporting fun, family friendly games like Mario Kart and Mario Party, both of which can be played with two or more players using the Joy-Con controllers.

NINTENDO ESHOP SETTINGS

In the Nintendo eShop you can set up a password to help stop your child or somebody else from accessing any sensitive information, such as bank account details. The options here include entering a password to access the eShop to begin with, when any saved credit card information access is attempted, or when PayPal is accessed. Choosing which areas are password protected helps ensure you're deciding what level of access is given on the device. For example, if you're happy to have your child browse the shop for games they might want, you can allow access to the eShop but introduce the password before a purchase is made ensuring no mishaps occur.

LIMITING PLAY TIME

By linking the app with the Nintendo Switch, you can set time limits and reminders when you think enough time has been spent playing. It also lets you see if a game is still being played and gives you the option to automatically put the console into sleep mode if the message is ignored. This should only be used as a last resort though as it could cause some friction between you!

SET PLAY TIMES

Another handy feature is the ability to set different playtimes for days of the week, allowing you to tailor play time around you and your child's schedules. This is great for setting boundaries and encouraging gaming as part of a healthy routine. It will also help your child organise with their friends when they can all be online.

SEE PLAY HISTORY

The Nintendo Switch Parental Controls app can also send a report telling you how much time your child spends playing each game. This is a great way to spot their favourite or most played games and might be a nice way for you to find out more about a title before talking to your child about it. It could also help identify any possible issues around playtime before they arise.

Meet our expert

Mark Foster has worked in the gaming industry for 5 years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGbible. Starting gaming from 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.

https://www.nintendo.com/switch/system/, https://www.nintendo.co.uk/Support/Parents/Safety/Keeping-your-child-safe/How-does-Nintendo-keep-your-child-safe--888083.html, https://www.youtube.com/watch?v=PLdWHOW9zqc, https://www.nintendo.co.uk/Nintendo-Switch/Nintendo-Switch-Online/Nintendo-Switch-Online-1183143.html

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 31.07.2019