Online Safety
A Parents Guide
## Contents

Online Safety: Engaging with Parents  
Page 3

7 questions to help you start your ‘conversation’  
Page 5

- Live Streaming  
Page 7
- Fake News  
Page 9
- Screen Addiction  
Page 11
- Online Bullying  
Page 13
- Catfishing  
Page 15
- Online Grooming  
Page 17
- Sexting  
Page 19

- The App Store  
Page 21
- Age Ratings  
Page 23

- Fifa (3+)  
Page 25
- Minecraft (10+)  
Page 27
- Fortnite: Battle Royale (12+)  
Page 29
- Houseparty (13+)  
Page 31
- Instagram (13+)  
Page 33
- Kik (13+)  
Page 35
- Reddit (13+)  
Page 37
- Roblox (13+)  
Page 39
- Snapchat (13+)  
Page 41
- TikTok (13+)  
Page 43
- Twitch (13+)  
Page 45
- Twitter (13+)  
Page 47
- YouTube (13+)  
Page 49
- Yubo (13+)  
Page 51
- WhatsApp (16+)  
Page 53
- LiveMe (17+)  
Page 55
- Grand Theft Auto – GTA (18+)  
Page 57

Momo  
Page 59
ONLINE SAFETY: ENGAGING WITH PARENTS

How can schools help parents?

1. Videos

VIDEO HAS BECOME AN ESSENTIAL PART OF THE ONLINE EXPERIENCE AND IS THE PERFECT MEDIUM FOR DELIVERING A MESSAGE QUICKLY AND EFFICIENTLY. 60% OF PARENTS TOLD US THAT THEY PREFER TO LEARN ABOUT ONLINE SAFETY VIA E-LEARNING VIDEOS THAT THEY CAN ACCESS IN THE COMFORT OF THEIR OWN HOME.

Source: National Online Safety Parent Survey - November 2018

2. Social Media

MOST PARENTS ARE ACTIVE ON SOCIAL MEDIA, EITHER DIRECTLY OR INDIRECTLY VIA FAMILY MEMBERS, USE SOCIAL MEDIA TO ENGAGE WITH YOUR COMMUNITY ABOUT ONLINE SAFETY, WHETHER IT'S SHARING RELEVANT ARTICLES/INFORMATION, ASKING QUESTIONS OR SIMPLY SHARING BEST PRACTICE. IT'S IMPORTANT TO REMIND PARENTS ABOUT THE IDEA OF YOUR SCHOOL BEING ON SOCIAL MEDIA AND TO ENCOURAGE THEM TO USE IT.

3. Closed groups / chat apps

CLOSED GROUPS ON PLATFORMS SUCH AS FACEBOOK AND WHATSAPP ARE IDEAL FOR SHARING MESSAGES AND UPDATES ON A REGULAR BASIS. IT ALSO REMINDS PARENTS OF ELIGIBILITY RULES AND ETIQUETTE GUIDES ABOUT WHAT CAN BE POSTED, AND INTRODUCE PROCESSES FOR APPROVING OR REFUSING TO JUDGE OTHER PEOPLE.

4. Posters and infographics

SHARING POSTERS AND INFOGRAPHICS TO PARENTS VIA YOUR WEBSITE OR SOCIAL MEDIA CHANNELS CAN BE AN EASY WAY OF SHARING ESSENTIAL ONLINE SAFETY INFORMATION ENGAGING AND MEMORABLE. A WELL-DESIGNED INFOGRAPHIC CAN CATCH THE EYE, PRESENT COMPLEX INFORMATION AND PRESENT IT IN A WAY THAT IS BOTH RELEVANT AND UNDERSTANDABLE TO YOUR COMMUNITY.

5. Email Newsletters

EMAIL COMMUNICATION IS GREAT FOR SHARING MORE IN-DEPTH INFORMATION FOR PARENTS TO LOOK AT IN ONE PLACE. IT IS A RELIABLE WAY OF KNOWING IF A MESSAGE HAS BEEN DELIVERED (AS YOU CAN TRACK IT). YOU CAN SEND MONTHLY NEWSLETTERS (OR MORE FREQUENT UPDATES TO KEEP PARENTS ENGAGED ON THE LATEST EMERGING TRENDS AND NEWS RELATED TO THE ONLINE WORLD AND EVOLVING RISKS.

6. Blogs

A BLOG IS A GREAT WAY TO DEVELOP A WHOLE SCHOOL CULTURE OF COMMUNICATION AND ALLOW PARENTS TO HEAR DIRECTLY FROM SCHOOL STAFF AND PUPILS ON TOPICS INCLUDING ONLINE SAFETY AND TECHNOLOGY TRENDS. WHY NOT CONSIDER HAVING A VARIETY OF AUTHORS, INCLUDING LEP, PUPILS AND PARENTS TO FORM A BALANCED VIEW. IT MAY ALSO BE WORTH RENLING A DEDICATED AREA ON YOUR SCHOOL WEBSITE TO ONLINE SAFETY.

7. Online learning

WE TYPICALLY SEE AN ENGAGEMENT RATE OF 10% OR LESS FOR IN-PERSON ONLINE SAFETY SESSIONS BETWEEN SCHOOLS AND THEIR PARENTS. TIME IS PRECIOUS AND ACCESSIBILITY IS IMPORTANT – ONLINE TRAINING TIPS MOST BOXES WHEN IT COMES TO MAKING INFORMATION READILY AVAILABLE TO YOUR ENTIRE COMMUNITY IN A REALLY ENGAGING AND INTERACTIVE WAY.

www.natonalonesafety.com  Twitter @natonalonesafety  Facebook /nationalonlinesafety  Phone 0800 368 8061

National 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 may 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?

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?

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 they spending time online right now. Asking them 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.

www.nationalonlinesafety.com  Twitter - @natonlinesafety  Facebook - /nationalonlinesafety  Phone - 0800 368 8061
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 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.

### What parents need to know about LIVE STREAMING

#### SIGN UP PROCESS & AGE RESTRICTIONS
Most live streaming apps have an 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 for an account. This also opens the opportunity for people to lie about their age to seem older or younger.

#### WHO IS WATCHING YOUR CHILD?
If your child's privacy settings are not set up effectively, anybody can be watching their live stream. 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 onlook, regardless of whether they know them.

#### LIVE CONTENT
As the streams are live, children can instantly be exposed to anything inappropriate. Most live streaming apps will have filters, rules and guidelines in place to ensure their services are monitored, but like any platform, the content that is uploaded is at risk of inappropriate content being sent to view. Bear in mind that a reporting system may not always work, which means your child may be further exposed to inappropriate content during a live stream.

#### RECORDINGS OF YOUR CHILD
Each streaming app and website that allows live streaming has different rules about how they store their live videos under "archive". For example, Periscope will be automatically deleted after 24 hours, but apps such as Facebook and YouTube allow the video to be posted on the app and will only be deleted once a user explicitly decides that. It is important to remember that 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 software and then shared on other platforms. Research conducted by the Internet Watch Foundation (IWF) discovered that approximately 12% of live streams were redistributed on other sites.

#### 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 pages. Anything can be streamed at any time and any place, including explicit content, pedophile content, and illegal behaviour. Most live streaming apps claim to monitor their streamers and will take action to stop any that do not adhere to their guidelines. However, with millions of live streams being streamed daily, it is extremely difficult to monitor them all.

#### GROOMING
There have been recent reports of paedophiles coercing children as young as ten through live streaming apps. Due to the anonymous nature and lack of identification needed to sign up to these apps, almost anyone is able to sign up and use the service. Users can use fake identities to sign up to these apps and stream videos. Recent research by the IWF revealed that children may be asked to do things and perform suggestive actions during their live stream by strangers.

### Top Tips for Parents

#### BE PRESENT
In a recent three-month period, the Internet Watch Foundation (IWF), 96% of streams showed a child on their own, either 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 a greater knowledge of what your child is doing during their live streams and who they are streaming to.

#### PROTECT THEIR PERSONAL INFORMATION
Your child may unknowingly give away personal information including their location. Talk to them about what constitutes 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 personal information.

#### TALK REGULARLY WITH YOUR CHILD
Ask your child which live streaming apps they are using and how they are using them. Are they watching live streams or making their own? What type 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 they should not be using the apps even if they are over the age limit. With live streaming being such a popular feature on apps, it is important that you are aware of the dangers associated with it in order to protect your child effectively.

#### 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 needs to set their privacy to be private. This will ensure that only their friends, followers or their friends, followers and friends of friends can view their stream. The settings vary from app to app, but it is important that when they go to stream, they set it as private.

#### PROTECTING THEIR ONLINE REPUTATION
What your child does now may affect their future opportunities, and it is important that they have a good understanding of this. As the online world is extremely interconnected, it may lead to the misconception that whatever happens in the video will disappear once the live stream ends. This is incorrect. Tell your child that their live streams cannot be undone and this 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 the videos further. For example, a live stream on Periscope, can be shared on Twitter and Facebook during the stream if the accounts are connected. While it may seem like a good idea to show the video to more people, the privacy settings may differ on each app, opening up the potential for unwanted videos to be shared. It is important to check the privacy settings on each app and where possible, only streaming on one app at a time in order to have greater control over who sees the live stream.
How to spot FAKE NEWS

WHAT IS 'FAKE NEWS'?*
Fake news can be false information, photos or videos purposefully created to confuse or misinform. It can also be genuine information that has been manipulated to deceive. It is important that we learn how to distinguish between real news and fake news.

DOES IT SOUND REAL?
Many fake news stories are written with appealing headlines and have content designed to create 'shock value' in order to spread like wildfire. Typically, fake news will include topics such as the 'death' of a famous person, company giveaways, news relating to supernatural events, or terror related posts that provoke a reaction. Have a look at other news sources to see if a story has been widely reported before sharing unsubstantiated claims. You can also check facts at websites, including snopes.com and factcheck.org.

CHECK 4 SPELLING AND GRAMMATICAL MISTAKES
Not always, but poor spelling, grammar and vocabulary on articles may indicate that an item is not from a reputable source. Be wary!

Read more than just the headline!
Some news sites will post stories with 'click bait' headlines to grab your attention and make you click on them. These headlines might not even be relevant to the story. Studies show that almost 60% of links that people have shared on social media have never actually been clicked before sharing, so it's really important that you read the article first before you share it to make sure the news is real.

Have you checked the URL? https://
Does the website address at the very top of the page look real? One of the easiest ways to spot suspect stories is if they're located on a news site with an odd domain name. So, check the URL. Some dodgy websites will try to incorporate a legitimate news source into its URL, such as www.theredbubble.co.uk, or will slightly misspell a popular website domain, e.g. www.bbc.co.uk.

Check the comments!
Have a read through the comments on a news story - either at the bottom of the article or on a social media share. Reactions and comments can often show if other people don’t believe the story is true, or whether someone has confirmed it is fake news. Of course, you can’t always know if a comment is real!

How long has the page existed?
Be wary if a story comes from a news organisation you have never heard of. Some hoaxers will set up a quick website to spread fake stories and so-called 'breaking news'. So, if a story with bold claims originates from a website that has only just launched, you would be wise to doubt its authenticity. There are online tools, such as the Internet archive, that display the approximate age of a website on the Internet and allow you to view how it looked before.

Who wrote it?
Make sure that the website that published the story is a credible source, i.e. a major news network or local paper which has the resources to fact-check published stories. If you get your news primarily via social media, always check the source and use caution if the story comes from a news organisation you have never heard of. If the article has a byline, you should be able to research to see if the writer is a genuine reporter by searching for them on Google.

Is it a joke?
While most fake stories are designed to make you believe them, it's important to know how to spot when the content has been written as a joke on purpose. Articles from joke news websites (such as 'The Onion' or 'The Daily Mash') are hugely popular on social media but some people may think their stories are real. Always read joke articles with a pinch of salt.
It can be challenging for parents and carers to know whether children are spending too much time on their devices. Furthermore, it’s even more of a challenge to know whether a child is addicted to the internet and social media. As technology is becoming more pervasive, children and young people are experiencing tech-related dependencies. Do we as parents and carers have the knowledge to identify and support children and young people who may be developing an addiction to their devices?

What parents need to know about SCREEN ADDICTION

SMARTPHONE ADDICTION IS A RECOGNISED HEALTH CONDITION

Children as young as 13 are attending smartphone rehab following growing concerns over screen time. There are now help centers in the UK which deal with screen addiction for children and adults showing the seriousness of device addiction.

IT CAN CAUSE SLEEP DEPRIVATION

7 out of 10 children said they had woken up on sleep because of their online habits and 60% said they had neglected school work as a result. It is important that children get the sleep they need in order to focus the next day.

CONFIDENCE, SUPPORT & ACCEPTANCE

The Children’s Commissioner report ‘Life in Likes’, explored how children aged 6-11 are using social media today. It showed that children are using their devices to speak to their online friends about their problems and seek acceptance and support, removing face to face interactions.

LOSS OF INTEREST IN OTHER THINGS

Your child may become less interested in anything that does not include their device. You may notice that your child is missing school time and generally being less engaged with other activities in the home. It is important to discuss this with your child as soon as you notice a behavioural change.

APPS CAN BE ADDICTIVE

Apps have been designed with psychological tricks to constantly keep grabbing your attention. One example of this is on the app Snapchat, where you can gain ‘streaks’ when interacting with your friends. If you don’t respond, you lose the streak. This addictive nature of apps aims to encourage children and keep them coming back for more.

Top Tips for Parents

LIMIT SCREEN TIME

In today’s digital age, technology is an important part of a child’s development so completely banning them from their device will mean they are missing out on a lot, including connecting with friends and family. Rather than banning them from using their devices, we suggest setting a screen time limit. Work out what you think is a suitable and healthy amount of time for your child to be on their device per week. Remember that your child may need to use devices for their school homework so only set screen limits on recreational time on their device. Once you have established these, have the conversation with them to discuss why you are implementing a screen limit. There will be other’s in your child’s friendship group who will not have screen limits set and will be sending messages when they do not have access to their phones.

LEAD BY EXAMPLE

Children model their behavior on their peers, so if their parents are constantly on their device, they will see this as acceptable behavior. Create a house rule and follow the same rules you have set for them. If you have asked your child to not use social media at the table, make sure you don’t. Try setting house rules that the whole family abides by.

LESS TIME MEANS LESS EXPOSURE

There are many risks associated with devices, such as cyberbullying, grooming, sexting, viewing inappropriate content etc. Less time spent on a screen means that a child will be less exposed to these risks.

ENCOURAGE ALTERNATIVE ACTIVITIES

It may seem like an obvious solution, but encouraging children to play with their friends, read a book, or playing outdoors will help them realize they can have fun without their devices. Playing football, team sports, camping, going for a walk or swimming are all healthy replacements for screen time. Try to join them in their outdoor activities to show your support.

MOBILE-FREE MEAL TIMES

Have you tried to settle your child by giving them a tablet at the dinner table or restaurant? This may seem like a quick fix to calm them down but in reality, it is encouraging them to use their device as a distraction from conversation and dealing with their emotions. We suggest removing all technology from the dinner table and having conversations with your family about how their day has been.

53% of children aged 3-4 go online for nearly 8hrs a week
79% of children aged 5-7 go online for nearly 9hrs a week
94% of children aged 8-11 go online for nearly 13.5hrs a week
99% of children aged 12-15 go online for nearly 21hrs a week

National Online Safety
www.nationalonlinesafety.com
Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061

A whole school community approach to online safety
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

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 singled out. 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.

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

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /nationalonlinesafety Phone - 0800 368 8061
What parents need to know about CATFISHING

In this technological era, making friends online and communicating with them are normal parts of life. Unfortunately, there are people out there who may try and exploit your trust. Catfishing is when someone creates a fake online profile to trick people into thinking they are somebody else. They assume a fake identity and go the extra mile to make their victim believe that they are exactly who they say they are.

WHY DO PEOPLE CATFISH?
The term ‘catfish’ was coined in a 2010 documentary about a man who developed an online relationship with a woman, only to discover the person he thought he was communicating with was someone else. Catfishers make up life stories and use photographs of unsuspecting victims to create fake identities. They will share life experiences, jobs, friends and photographs to the fake accounts. The aim of the perpetrator may be to lure victims into a sexual relationship, but they can also be part of social engineering to trick people out of money. After building trust and developing an online relationship, a catfisher may ask for cash for a loan, money for travel, or some other form of payment.

OTHER CONCERNS & WORRIES
Catfishing can escalate very quickly. As someone executing a catfishing scam is looking to achieve a goal - whatever that may be - they are likely to want to get things moving as quickly as possible. The victim may be encouraged to develop a relationship faster than they are comfortable with. In addition to this, people who create fake identities could also be taking the victim’s photos and pretending to be them. It is common for fraudsters to post pictures stolen from social media sites, including Facebook and Instagram.

HOW TO SPOT CATFISHING
Profile pictures and other photos that are posted can be big indicators. To avoid revealing their real identity, a catfisher may use ‘stock’ images of models, other people’s photos or photos in which it is difficult to see their face. They may try to limit chat to text-based messaging and anything involving video is likely to be shunned for fear of revealing their true identity. Through the course of conversation, there may be inconsistencies with what is said, or instances of people being very vague in response to specific questions about themselves.

Top Tips for Parents

MONITORING & CONVERSATION
Encourage your child to talk to their trusted adults about anything that has made them feel uncomfortable online, particularly if someone they don’t know has contacted them. Remind them that they should not accept friend requests or communicate with anyone they don’t know online, and to ask a parent or carer if they are unsure. It is also very important to closely monitor their internet usage so you are aware of who they are communicating with, especially if they are being secretive. Have regular and honest conversations with your child about what is safe to share with people online; the importance of keeping private information private; and that anything that could identify them should not be shared online.

PRIVACY & SECURITY
Go through your child’s security and privacy settings thoroughly to ensure that their online profiles are set to private. This means that only friends can see their profile and can contact them. It may also be a good idea to check through your child’s friends list with them - do they know and trust everyone on the list? In some cases it is difficult to stop young people from talking to new people. In these circumstances, encourage your child to be curious and ask lots of questions rather than rely on the information given in someone’s online profile. Do they have any mutual friends? If not, how did that person find them and why did they reach out? It’s vital that they know never to arrange to meet up with people they meet online, and never to send money to them - either their own, or from your account.

BE ALERT & REPORT
Make sure that you and your child are aware of how to report and block accounts on all platforms that the child uses. You can report fake accounts and block users to prevent them from viewing your child’s profile. If you are concerned that someone is using your child’s photographs for their own benefits, you can check by using Google’s image search. You can upload a photograph and Google will show related images used on other websites. This will show you if anyone else is using photos that your child has previously shared online. If this is the case, you need to report the user directly to the platform. If you suspect that any fraudulent, illegal or inappropriate activity has taken place, you should report to the police immediately.

A whole school community approach to online safety
www.nationalonlinesafety.com
Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061

National Online Safety

WARNING! Catfishers will target ANYONE OF ANY age
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, shares 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, Livmo, 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 parents expect groomers to be adults posing as children, but this is not always the case. Data from the 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.

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.

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 do know them. 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 casual 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, including 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 your child is in immediate danger, call the Police on 999 or NSPCC on 0808 800 5000.

© National Online Safety Ltd
This is not a prescribing guide. Please always check with the app’s support information to see if your security and advance comments are approved.

www.nationalonlinesafety.com
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 16, with police forces in England and Wales recording 6,238 under-16s under “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 Children and Young People Act 1999, the Serious Crime Act 2007 and the Sexual Offences Act 2003.

REGRETTING THEIR ACTIONS
Although some children are motivated by the exchange of images and videos, and may subsequently regret their actions, the damage is already done.

CHILDREN THINK IT’S HARMLESS
Many young people see exchanging naked or semi-naked images as an easy way to show someone they like and trust them, or as a way of taking control of the situation. But they may not realise the consequences of sharing personal information and how it can be potentially harmful to them in the future.

BULLYING, COERCION & BLACKMAIL
Your child may feel pressured into sexting, so they don’t come across as boring, or believe they’ll be shown something they can’t find anywhere else. They may feel under pressure to give in to repeated requests or feel obliged to share sexual images and messages. Sexting can also appeal to young adults to the risk of being exploited by paedophiles or sexual predators, who then use images to entice 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 enlarged 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 ‘exchanging’ and explore the consequences of sharing something. 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’re approachable and understanding.

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 may be available to everyone. They may end up where the whole world can access them. Even if they completely trust someone, other people using their phones might accidentally see it. And, later in life, it may affect their online reputation, especially for universials, employers or future partners access the imagery.

HOW TO REMOVE IMAGES
If an image has already been shared, either by your child or yourself, you 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 contact 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 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:
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 in 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 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, thereby allowing a higher percentage of apps that infect devices with malicious code 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 pops to the account organizer. 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, 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 iPad 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 2 and under, 4 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
Adviso 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 apps 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 a good indication.

Spot fake reviews
When checking the consumer reviews within the app store, make sure they aren’t vague and generic, or overly enthusiastic, as some developers will try to manipulate their app’s position 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.

Sources:

National Online Safety
A whole school community approach to online safety
www.nationalonlinesafety.com

Email us at help@nationalonlinesafety.com or call us on 0800 368 8061
What parents need to know about AGE RATINGS

If you have children, it is understandable to have concerns about the films and TV shows they watch, as well as the games they play. In this guide, we take a look at the two official ways you can assess if a particular title is suitable for your child. Both the BBFC and PEGI have search facilities on their websites that can be used to look up individual titles so you can check their ratings.

**RATINGS FOR FILMS, TV & MUSIC VIDEOS**

Since 1912, the BBFC (British Board of Film Classification) has informed UK residents of the age suitability of films, TV and music videos - providing parents with the information needed to assess whether or not it is appropriate for their child's age. This applies to cinema releases, DVDs and streaming video services such as Netflix.

**WHAT ARE THE BBFC RATINGS?**

BBFC ratings are broken down into seven age categories:

- **U** Universal, suitable for all ages
- **12A** Suitable for people aged 12 and over
- **12** Suitable for people aged 12 and over, any game accompanied by an adult
- **15** Suitable for people aged 15 and over
- **18** Suitable for people aged 18 and over
- **BBFC Informational Rating**
- **BBFC Children's Rating**

Accompanied with the age suitability rating, BBFC also provide an additional warning regarding the content and what to expect, such as swearing, sexual content, violence and anything you may consider to be inappropriate for your child. In addition to this, the content is also rated in three levels: frequent, mild or strong.

**LIMITATIONS OF BBFC RATINGS**

It's important to note that there is no obligation on streaming video services to use or display BBFC ratings. Due to this, we advise that you check the rating online before your child streams the content. It may also be a good idea to watch the content first yourself or discuss it with other parents to help you decide whether or not it is suitable for your child.

**RATINGS FOR GAMES**

PEGI (Pan European Game Information) is a content rating system that ensures all video games are labelled with a minimum age recommendation. These age recommendations are based on the types of content featured within a game. With each game, PEGI also provide a content descriptor that indicates the potential issues and concerns, including sex, violence, bad language and drugs.

**WHAT ARE THE PEGI RATINGS?**

PEGI ratings are split into age restriction and content descriptors. Additional content descriptors help parents and children to understand the type of content featured within a particular game, including sex, fear, bad language, discrimination, gambling, drugs, violence, and in-game purchases. In combination, the two different ratings can provide a good level of information to help make informed decisions regarding the suitability for your child.

**PEGI age ratings are broken down into five categories:**

- **3**
- **7**
- **12**
- **16**
- **18**

**PEGI content descriptors are broken down into eight categories:**

- **Violence**
- **Life**
- **Abuse**
- **Bad Language**
- **Sex**
- **Discrimination**
- **Gambling**
- **Drugs**

**LIMITATIONS OF PEGI RATINGS**

It's possible for young people to buy games online without a required proof of age, opening them up to age-inappropriate content without you knowing. We advise that you regularly monitor your child's gaming activities and maintain a honest and healthy dialogue with them about the online world.

**PARENTAL CONTROLS**

It is a good idea to put in place parental controls for all online accounts which your child may use to purchase or download online games e.g. The App Store, Google Play Store, PlayStation Store and Microsoft Xbox Store etc.

Source: www.bbc.co.uk

A whole school community approach to online safety

www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8051
What parents need to know about

FA

FAKE EMAILS, SCAMS AND COPYCAT WEBSITES

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’.

BUYING ADD-ONS

In-game purchases are 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.

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 series of 30 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.

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

CONSTANT SERIES REFRESHES / WHAT TO DO?

As a parent, the implications of this really depend 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.

IN GAME CHAT

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.

FAKE EMAILS, SCAMS AND COPYCAT WEBSITES

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’.

BUYING ADD-ONS

In-game purchases are 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.

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 series of 30 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.

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!

www.nationalonlinesafety.com
Minecraft is played by millions of children around the world, who use their imagination to build three-dimensional worlds with virtual building blocks in a digital, pixelated landscape. It is classed as a ‘sandbox game,’ which means players have the freedom to build their own creations with ‘blocks’ they collect and also have the opportunity to explore other people’s creations with their characters. Players can choose from thousands of different servers to join, which are created by other players, making every experience of Minecraft unique.

**What parents need to know about MINECRAFT**

**GROOMING**
As the majority of users who play Minecraft are children, this makes it an appealing gateway for groomers. It has been reported that some users have created worlds in Minecraft to lure young people into a conversation to ask for explicit photos. There have even been more serious cases in which children have been persuaded to meet these people in real life.

**CYBERBULLYING & GRIEFING**
In multiplayer mode there is a live chat feature which allows players to talk to other players through text. This chat functionality includes basic filtering to block out external links and offensive language being shared, but varies between each server. Griefing is when someone purposely upsets another player during the game. This can be done by ruining somebody’s creations or generally doing something to spoil gameplay for another. Essentially, ‘Griefing’ is a form of cyberbullying and can be extremely frustrating for players.

**COMMUNICATING WITH STRANGERS**
Minecraft incorporates thousands of servers to choose from which are a single world or place created by the public and allow users to play the game online or via a local area network with others. No two servers are the same and each has its own individual plug-ins which are controlled by the creator. This means that some servers will allow communication with strangers.

**VIRUSES & MALWARE FROM MODS**
There are several websites that offer downloadable ‘mods’ which modify gameplay in a number of ways. Most of the mods will be safe to use, but as they have been created by the public they will often contain viruses that can infect your child’s device and potentially try and find personal information about you or your child.

**AGE RESTRICTION & ‘FANTASY VIOLENCE’**
According to the ‘Entertaining Software Ratings Board’ (ESRB), Minecraft is suitable for users aged 10+. Due to its ‘Fantasy Violence,’ the ESRB states that this rating has been given as players can engage in violent acts such as setting animals on fire and harming them with weapons. Mild explosions are occasionally heard as players use dynamite to fend off creatures and mine the environment.

**CHILDREN MAY BECOME ADDICTED**
As with other games, Minecraft is a game where players can keep returning with constant challenges and personal goals to achieve. Children may find it difficult to know when to stop playing, becoming absorbed in the game and losing track of time.

---

**Top Tips for Parents**

**DISABLE OR MODERATE CHAT**
To avoid potentially inappropriate comments in a live chat, you can follow these steps to turn live chat off: 1. Select ‘Options’ 2. Toggle the Chat button to ‘Hidden’ or ‘Command Only’. Bear in mind that the chat feature is also where your child can enter commands during the game, so this may restrict their gameplay.

**SCAN ‘MODS’ FOR MALWARE**
Minecraft ‘mods’ add content to games to give extra options to interact and change the way the game looks and feels. However, although ‘mods’ can bring fun for a child, it’s important to consider that downloading and installing mods could potentially infect their device with a virus or malware. In 2017, security company Symantec stated that between 600,000 and 2.5 million Minecraft players had installed dodgy apps, which hijacked player’s devices and used them to power an advertising network. It’s an easy mistake for anyone to make, especially on a device that your child plays Minecraft on and make sure it’s regularly kept up-to-date.

**SET TIME LIMITS**
With ‘Gaming Disorder’ becoming an official health condition, we suggest setting a reasonable time limit when playing Minecraft. Parents can use parental controls on devices to limit the time a child plays games. It is worth having a conversation with your child to understand which ‘modo’ they are playing the game. This may help you decide on the amount of time you would like them to play. For example, a mini game will have an ‘end’, but this will depend on how long the game creator has made the game last. In ‘Survival Mode’, the game has no end and so there is no goal to be achieved other than the child’s own e.g. after they have built something.

**CHOOSE SERVERS CAREFULLY**
To protect your child from engaging in conversation with strangers, advise them to only enter servers with people they know and trust. Your child can also create their own multiplayer server and share this with their friends, which is safer and more controlled than joining a stranger’s server.

**Scan your device**
Before your child plays any Minecraft servers, you should scan your device to ensure your child is not infected with malware.

---

Sources:

**This is an independent online safety guide and is not an official Minecraft product. This guide has not been approved by nor is it associated with Mojang.

© National Online Safety Ltd
The above information gives general advice which can be varied based on the app’s or game’s support information to see if your security and privacy concerns are addressed.

National Online Safety
Top Tips for Parents

---

www.nationalonlinesafety.com
FORTNITE: BATTLE ROYALE

What parents need to know about

MICROTURANSCTIONS
Newly featured items are released daily and are only available to purchase within 24 hours of their release. These are cosmetic items, like skins, gliders, and emotes, which change the characters appearance. They do not affect gameplay. Parents who purchase the game have full use of them in the future. The developer is aware of the game being endorsed by hackers. Also, available to purchase in the game is a "Battle Pass" and "Fortnite Battle Pass" related ones. Hackers can take part in a series of challenges, receiving more rewards (cannons) by progressing through different tiers. Whichever rewards they achieve can then be used in the game.

HACKER ATTACKS
News site Forbes stated that it had seen "loans" of online accounts from hacked players. These accounts had been compromised by hackers, who had gained access to user's accounts in the game and had used them to drain the contents of pounds in fraudulent charges.

NO PROOF OF AGE REQUIRED
Signing up to the game is relatively simple. Users have the option to login with either their Facebook or Google accounts or their email address. When signing up with an email address, there are no age verification procedures. As long as it is under the age of 12, it is important to check whether your child has the game downloaded.

TALKING TO STRANGERS DURING SQUAD MODE
Interacting with other players in the game is part of the fun for players. It can help with player development and make the game more enjoyable. However, it can also make it difficult for parents to hear exactly what is being said and make it inappropriate for children. Fortnite includes really good reporting features for players who are cheating or misbehaving, and this works 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, which does require a fee.

IT CAN BE ADDICTIVE
Games can last around 20 minutes but this varies according to the game. Children may find that they lose the game and will want to continue playing until they achieve their desired result. The competitive nature of the game may make it difficult to stop them playing.

IT CAN BE PLAYED ON THE GO
The game was released on mobile devices in April 2018, meaning it can be played without the need for a home games console. Some schools have reported that the game is distracting their students and has caused problems. As the game is available outside of the home, parents may not be aware of how long their child is playing this game.

LIMIT GAME TIME
Parents can use parental controls on XBox and PC to limit the time a child is playing games on these devices. Be aware that the game is available on iOS and can be found available on all mobiles. With this in mind, it is worth having a conversation with your child to discuss how long you would like them to play the game for. Even though the games last around 20 minutes, it may be difficult to take them away from the game and, in this case, it may be worth imposing a limit on the amount of matches they play rather than a time limit.

PREVENT YOUR CHILD FROM TALKING TO STRANGERS
There is an option to turn off the voice chat feature, which means your child wouldn’t be able to talk to anyone, including their friends. However, they would still be able to use the in-game chat and have other players conversations. To turn off voice chat, open the Settings menu in the top right of the main Fortnite menu, and then go to the options. Open the Audio tab at the top of the screen. From there, you can turn off voice chat.

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 conversations with them about scams and how they should never share their username or password with people in order to gain anything for the game.

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 restrict spending, you could consider chasing up the purchase. These can be purchased in specific amounts, which will allow you to restrict the amount your child spends and removes the need for a credit card to be used with their account.

AGE RESTRICTIONS
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 realistic and graphic looking violence towards fantasy characters is allowed. Any violence towards human characters must look unrealatively unless it consists of only minor or trivial injury such as a slap, making the game suitable for children aged 12 and over.

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. If they report a player in-game when spectating them.

USE A STRONG PASSWORD
It may seem simple, but it is important that your child selects a strong password when creating an account, particularly if a credit card is being used to make purchases. This will help protect your account and help reduce the risk of their account being hacked.

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

http://www.bbc.co.uk/uk/ireland/games/45236075
fortnite accounts hacked how to protect your and what to do if you've been compromised/14423795739
Houseparty is a live streaming app described as a face-to-face social network where people drop in on each other to video chat, leave messages and hang out in groups. In the UK alone, there is an estimated 1.3 million people using the app, more than half of which are under the age of 24. Houseparty is available for iOS, Android and Mac OS, and it's important to note that children under the age of 13 must have a parent's permission to use the service. Therefore, no proof of age required to create an account.

**What is Houseparty?**

Houseparty is a live streaming app described as a face-to-face social network where people drop in on each other to video chat, leave messages and hang out in groups. In the UK alone, there is an estimated 1.3 million people using the app, more than half of which are under the age of 24. Houseparty is available for iOS, Android and Mac OS, and it's important to note that children under the age of 13 must have a parent's permission to use the service. Therefore, no proof of age required to create an account.

**How do young people use it?**

Each time the app is opened, your child will be instantly connected to other users who are also on the app. Users can invite friends to join their group and create private group conversations of up to eight people at one time. Each time a person joins, the screen splits to show everyone who is part of the conversation. Your child can add contacts via phone numbers, search for their usernames, and share a link to their profile. They can have as many rooms as they want and move from chat to chat by panning across the screen. Along with the functionality comes a few associated risks to be aware of...

**What parents need to know about Houseparty**

- **STRAngER DANGER**
  - Friends of friends can join conversations on the platform without the need or be connected to or known by all the users in the chat. Houseparty calls this feature "Stranger Danger". While it doesn't alert users when someone is not their friend, it also suggests strangers might be a reason for concern when attempting to deliberately mislead others by using false names or usernames.

- **SEXUALISED MESSAGES**
  - People may use live streaming apps such as Houseparty to engage in inappropriate or illegal activities. There have been public reports of minors being targeted by adults, including one incident where two Ukrainian children aged 13 and 12 were sexualised in a chatroom before they were placed in the app.

- **CONTENT BEING SHARED**
  - The 'social' feature lets users share moments from their Houseparty conversations by recording and sharing 15-second clips of chats. They also have the option to save those moments to their gallery. For privacy reasons, the company recommends that parents should be informed before sharing.

- **IN-APP PURCHASES**
  - By tapping on the icon you can play a game called "Friends Up!" where the player chooses clues to describe someone or something and the other players guess. Three cards are included for free but additional decks cost 99p. Parents should be aware of this when allowing their child to use the app.

- **SAFER CONVERSATIONS**
  - With live streaming being such a popular feature on apps, it's important that you're aware of the dangers associated with it in order to protect your children effectively. Have regular and honest conversations with your child about what apps they are using and how they are using them. It may be a good idea to have your child show you how they use Houseparty and how to navigate through the platform so you are aware of how it works.

- **PROTECT THEIR PRIVACY**
  - Your child may unknowingly give away personal information during a live stream, including their location. Talk to them about what constitutes personal information and encourage them to 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 personal information. Check your child's privacy settings thoroughly. You have the option to opt out of certain uses and disclosures of personal information, such as turning off the app's location sharing option.

- **OVERSHARING PERSONAL INFORMATION**
  - Children often don't understand the risks involved in giving out too much personal information in a live stream or within their profile. They may also be less protective of personal data online. For example, if someone were to view a live chat could be bullied by revealing sensitive information about where they live or go to school without realising.

- **CYBERBULLYING**
  - Cyberbullying is when people use technology to harass, threaten, embarrass, or target another person. Groups can be used by dueling, mocking or hurtful comments which may cause damage or be humiliating to the other person. Children from distant friendship groups within the platform may make your child feel safe and left out intentionally.

- **LOCK ROOMS**
  - In regards to communicating with users on the platform, we advise that you child uses the 'lock' feature to make their conversations private. This means that other users, especially strangers, can't join their conversations.

- **BE PRESENT**
  - A study conducted by the Internet Watch Foundation (IWF) found that 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 they could be present for it. This will give them a greater understanding of what your child is doing during their live streams and who they are streaming to.

- **REPORTING AND BLOCKING**
  - If your child faces a problem while using the app, they can report or block the user directly on the user's profile. A prompt will pop up allowing them to report issues immediately by clicking on the report now button. They also have the option to report and block users directly on the user's profile.

**Top Tips for Parents**

- **SAFER CONVERSATIONS**
- **PROTECT THEIR PRIVACY**
- **OVERSHARING PERSONAL INFORMATION**
- **CYBERBULLYING**
- **LOCK ROOMS**
- **BE PRESENT**
- **REPORTING AND BLOCKING**

**Sources**

[https://www.thetimes.co.uk/article/houseparty-the-chat-app-that-sweeping-through-facebook-helps-skm](https://www.thetimes.co.uk/article/houseparty-the-chat-app-that-sweeping-through-facebook-helps-skm)


**A whole school community approach to online safety**

www.nationonline.safety.com

Email us at help@nationonline.safety.com or call us on 0800 368 8061

SEE ALSO: LIVE STREAMING GUIDE FOR PARENTS
Instagram is an image and video sharing app that allows users to share moments with the world. The app has a live streaming feature and additional add-ons, such as ‘Boomerang’, ‘Hyperlapse’ and ‘Layout’, which can be used to enhance their feed. Users can choose to add filters and make adjustments, such as brightness / contrast to their photos. To make their content more ‘searchable’, users can include hashtags in their uploads to make them easier to find.

What parents need to know about

INSTAGRAM

LIVE STREAMING TO STRANGERS
The live stream feature on Instagram allows users to connect with their friends and followers in real-time. Followers can comment on the video during the broadcast (which can be turned off in the settings). If your child has a private account, only their approved followers can see their story. It is important to note that they still may have followers that they do not know, which means they could be live streaming to strangers. A public account allows anybody to view their story. We suggest that your child goes through their followers list and blocks anyone they do not know. An additional risk with live streams is that your child may do something that they regret. This could be captured by a viewer taking a screenshot and then shared around the Internet.

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.

DAMAGE TO CONFIDENCE, BODY IMAGE & MENTAL HEALTH
When people use filters on their photos on Instagram, it can set unrealistic expectations and create feelings of inadequacy and low self-esteem in children. Children may strive for a comparable number of ‘likes’ to a realistically edited with the risk of drastically lowering your child’s confidence or sense of worth.

PHOTO / VIDEO SHARING
Posting photos and videos is Instagram’s biggest selling point, but with sharing comes risks. 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 not set to private, anyone can access their account and see their location.

LOCATION TAGGING
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.

HIJACKED HASHTAGS
Like Twitter, hashtags are also an extremely prominent tool in Instagram and with that comes dangers for your child. 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 certainly shouldn’t be exposed to.

INTEGRAM TV
Instagram TV works similarly to YouTube. Users can watch videos from their favourite accounts on the platform, or create their own channel and post their own videos. It’s important to note that anyone can create their own Instagram TV channel and you don’t have to be friends with a person to follow an account and watch their videos. Ultimately, features are encouraging users to spend more time on the app, therefore it’s important to set time limits and ensure their devices are not disturbing their sleep and performance at school.

Top Tips for Parents

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 purchase; this will also help prevent unauthorised purchases. This can be added in the payment settings tab.

RESTRICT MESSAGES
If your child’s account is not set to private, anybody can message them and reply to their stories. If they do wish to keep their account public, we strongly recommend changing the message reply settings to restrict who can message them.

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.

FILTER INAPPROPRIATE COMMENTS
Instagram announced on 1st May that they now have an anti-bullying filter on the app. This new filter hides comments relating to a person’s appearance or characters, as well as threats to a person’s wellbeing or health. The filter will also alert Instagram to reported problems so they can take action against the user if necessary. This is an automatic filter but it can be turned off. Make sure this is turned on in the app’s settings.

TURN OFF SHARING
Even though this feature will not stop people from taking screenshots, it will stop others from directly sharing 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.

National Online Safety
www.nationalonlinesafety.com
Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061
Kik (or Kik Messenger) is a free messaging app used by 300 million people worldwide that lets users exchange messages, photos, videos, GIFs and webpages via a Wi-Fi connection or data plan. Kik is unusual in that your child can sign up without a phone number and then find and message other people via just their username. Kik is aimed at anyone aged 13 years and older — the app says teens between 13 and 18 years old will need parental permission but it does not verify ages.

At parents need to know about Kik

Child Sexual Exploitation & Grooming
Police in the UK have warned that Kik has featured in 'more than 1,100 child sexual abuse cases in the last five years' and that 'abuse is risk' on the app. Users are required to set up their own child sexual exploitation, grooming, and image violations. Kik has also been identified by the NCPC as being used by sex predators, and they say it is responsible for several recent incidents involving children including the murder of a 13-year-old girl by a man she met via Kik.

Fake or Anonymous Profiles
What makes Kik unique is the fact that messaging apps is the fact that it requires a phone number as it works through Wi-Fi. Instead, it uses an anonymous name or profile. This can lead to the collection of personal information with others on Kik, but on the flipside, this makes it far easier for people to connect and even create fake personas.

Sexual Predators
Some people may use Kik with the intention of targeting children. Typically, this is a predatory person randomly met and they may pose themselves as a friend also understands a child's age. They may be given personal information and it is possible that the child may be manipulated by a stranger into doing reportable or illegal activities, and maybe even meet in real life.

Choosing a Username
When setting up a Kik account, ensure that your child knows the importance of a secure username and why it shouldn't contain ANY data that can be used to identify your child, their family, or their friends. They should try to use a username that is easy to remember, but that can't be easily associated with any personal information or photographs.

Sharing Your Contacts
While Kik allows you to share information with others on the app, it also requires that you accept a friend request before any information is shared. This means that anyone you add as a friend or that sends you a message can be blocked or reported at any time.

Avoiding Unexpected Images
Kik encourages users to report any inappropriate content they may come across. If you encounter any impropriety, you can report it to Kik's customer service team, which will then take appropriate action.

Using a Valid Email
According to Kik, it's important for users to provide a valid and accurate email address when registering their account. This will help to verify the user's identity and make it easier to access important emails from the service, such as a link to reset their password.

Muting or Leaving a Chat
If someone has sent something inappropriate to you through Video Chat, they can either leave the chat or mute the Video Chat. To mute the Video Chat, you must be the person who is receiving the messages and you can do this by clicking on the mute icon in the chat window.

Communication is Key
If your child sees something disturbing, inappropriate or concerning, encourage them to talk about it. Parents and guardians should always be there to help them if they need it. If they start acting differently or normal, gently ask them why.
What parents need to know about Reddit

Sub-Reddits
Each community (known as a sub-reddit) has its own self-moderator and its own set of rules. There might be opportunity for your child to see inappropriate content or something they might 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.

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 right-to-use moderation, so even the most open-minded of people may find deeply offensive content. Reddit generally provides a list of channels of the types of content which is acceptable. Some members choose to avoid certain content, 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 mock what they are talking about by swapping 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 1000000% (100%) (10%).

ContenT Bias And Fake News
Subreddits can be particularly prone to bias. 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 others who have similar interests, some will choose to be troll and abuse, or by your child encountering unsavoury subjects, Reddit users can also send each other other private messages, so there is a danger of your child receiving inappropriate or unwanted communication.

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 again and not to take something at face value. Just because something is said by someone on Reddit, it doesn't mean it's true. Remember that links people post and the comments they leave will cover the full range of 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 be careful 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/nosubscription/comments/827mp/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 new features and privacy concerns are addressed.
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 to remove games from the platform Roblox relies on people reporting negative/violent content.

**CHATTING & 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 that 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 and enables 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 ability 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 via a PayPal account. To withdraw money, users need to be over 13, have a PayPal account and have paid for the Roblox premium subscription.

**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 information if they are, advise them to set them to private or remove them from their account. This will ensure that nobody will be able to 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.

**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 generally doing something in the game to spoil their gameplay. Essentially, 'Griefing' is a form of cyberbullying and can be extremely frustrating and upsetting for players.

**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 restrict spending, we suggest using a games console gift card. These can be purchased in specific amounts, which will enable you to restrict how much your child spends and remove the need for a credit/debit card to be used with their account.

**DISABLE IN-GAME CHAT**
Roblox is great for children to play together and chat to each other. However, if you want to completely turn off in-game chat for your child (meaning they cannot 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.

**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 and agreements. 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.

---

**SOURCES**
Organisations and websites included in the Learning Library ©2019 NHS Commercial, Roblox and the Roblox logo are trademarks of Roblox Corporation. Roblox is a trademark of Roblox Corporation and is not affiliated with or endorsed by us. This content is not endorsed by Roblox. Also, copyright laws may preclude our use of certain images in this USA and other countries.

www.nationalonlinesafety.com
Snapchat is a photo sharing app for mobile phones and tablets. The app allows users to share images, videos and chat with friends. 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

EXPOSING YOUR CHILD'S ACTUAL 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 'if you share a message with 'Our Story' it can still be shared 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.

LENS EXPLORER

The 'Lens Studio' on Snapchat gives users the freedom to use their imagination to design their own filters for themselves and others to use. Snapchat states that the lenses users create 'must comply with our Lens Studio Submission Guidelines and Community Guidelines and must be appropriate for Snapchatters ages 13.' The 'Lens Explorer' in the app now enables users to choose from thousands of these creations to alter their snaps. Anyone can create a lens for Snapchat, which gives opportunities for age-inappropriate content to be uploaded.

SCREENSHOTS & SAVED MESSAGES

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 this or not be aware of it. It is not necessarily a compromising image or message to somebody who they think they trust. They may also accidentally send an image or message to somebody who they do not trust. Simply by pressing and holding a message, the user can stop the message they received, which can be screenshot or used against them at a later date.

SNAPSTREAKS & ADDICTION

'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

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 screenshot, 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.

SNAP ORIGINALS

Through 'Snap Originals,' users can watch content which has been created by Snapchat on the app, including comedy shorts, drama, news and more. Additionally, there are now lenses and filters available, inspired by the 'snap originals' shows. This is another feature to encourage addiction.

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 screenshot. 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, follow the onscreen instructions. 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 to 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 core 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'

'Snapchat' has fixed 'Quick Add' in the latest update of the app. This is based on mutual friends or if their number is in their phone book. Parents can stop this feature from appearing on 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 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.'

National Online Safety

www.nationalonlinesafety.com

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


https://nossafety.net/snapchat-parent-review | BIT.com | Independent.co.uk
What parents need to know about TikTok

**BEING INFLUENCED**

More than one third of children aged 6-17 consider 'social media stars' to be among their top role models. There are millions of creators on TikTok, showcasing their talents, moments and knowledge. From singing to dancing to start-up and comedy skits, which receive thousands of likes and comments from around the world, quickly turning people into 'stars'. There is the danger that children may develop unrealistic expectations of how they should look and behave on the app to become the next 'star'. They may have feelings of inadequacy and low self-esteem or become swept away by certain opinions.

**CONCERNING CONTENT**

Some of the outfits and dance moves in videos can be overly sexual and provocative. There have also been reports of users sharing concerning content, such as videos that promote_normalize_porn, self-harm and violence.

**DANGEROUS TRENDS & CHALLENGES**

On TikTok, there are many 'trending challenges' and hashtags that users can copy or build upon, and sometimes, these challenges can pose risks to young people.

**INAPPROPRIATE SONG LYRICS**

TikTok lets users lip-sync to their favourite songs and produce their own music videos. Some of the music choices contain swear words or sexual themes. So not only can children be exposed to potentially inappropriate content but they can broadcast themselves miming or singing these lyrics.

**IN-APP PURCHASES**

Of course, as with many apps, there's a paid element to TikTok. Users can pay virtual coins to exchange for virtual gifts - for example, if they like a specific video, your child can use coins to purchase emojis to throw on screen. These can be expensive and easily purchased. There is the option to buy 10,000 coins for £97.99 with a one-click buy button.

**ANYONE CAN SEE YOUR CHILD'S CREATIONS**

TikTok encourages users to share their passion and creative expression through their videos and while something may seem fun at the time, videos can get into the wrong hands and cause embarrassment. In the future, if posted publicly, anyone in the world can see your child's homemade music video and potentially cause bullying within personal friendship groups or even online.

---

**Top Tips for Parents**

**TALK ABOUT THE PITFALLS OF OVERSHARING**

Encourage your kids to always think before they do, say, like or post anything online, explaining that their 'digital footprint' can shape their online reputation and the way that other people see them. Something they may find funny and entertaining now may impact them in the future. Talk about how to deal with peer pressure and how doing something they think will impress others could affect them.

**HANDLING CRITICISM**

While it's natural to see your child being creative and expressive and bonding with people with similar interests, they need to be aware that not everyone will be supportive or nice. Comments can be negative or even cruel. Make sure they know how to comment respectfully and handle negative feedback. In the app's Privacy and Safety settings, your child can decide who can react to their videos, who can comment, and who can sent them private chat messages. We suggest turning these settings on if your friends can interact with their posts.

**SIGNING UP WITH THE CORRECT AGE**

When signing up to TikTok, you are prompted to input your birth date. If your child inputs their age as under 13, the app will not allow them to sign up or log on for 24 hours. The app is intended for users aged 13+, so explain that the setting is there for a reason: to keep them protected from online dangers. It is actually possible to watch TikTok videos without creating an account. It is important to talk to your underage child has downloaded the app to their devices.

**USE THE 'DIGITAL WELLBEING' SETTING**

If you're concerned about the amount of time your child is spending on TikTok, in the app's settings, you can switch on a feature called 'Digital Wellbeing'. This includes 'Screen Management' to limit the amount of time your child spends on apps.

**SET THE ACCOUNT TO PRIVATE**

This means that only people who you and your child approve of can see their content. To make an account private, tap the three dots at the top right of the screen to access settings, click 'Privacy and Safety', scroll down until you find 'Private Account' and turn this setting on.

**REPORT INAPPROPRIATE CONTENT**

If you see something on TikTok that is inappropriate, they can report it in different ways within the app. They can report an account, video, comment or chat conversation by simply tapping 'Report'. In the app's 'Digital Wellbeing' feature, there is also an 'Enhanced Restricted Mode', which limits the appearance of videos that may not be appropriate for all audiences.

**AVOID IDENTIFIABLE OBJECTS**

To ensure there's no way of anyone tracking your child's location or identity, make a clear to them that they should never film a video in their school uniform or near a landmark that gives away where they live.

**DISCUSS IN-APP PURCHASES**

To lower the risk of your child making accidental in-app purchases, teach them exactly what in-app purchases are and the risks of making them without permission. Tell them that they are not essential to enjoy the app and that if they want to make a purchase, they should always ask you beforehand. In the app's 'Digital Wellbeing' feature, there is the option to disable the function of purchasing coins and sending gifts.

---

**National Online Safety**

**NOS**

---

**TOP TIPS FOR PARENTS**

---

**SOURCE:**

National Online Safety Ltd

---

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

---

https://www.nationalonlinesafety.com
What parents need to know

Twitch is a gaming-focused live-streaming service, owned by Amazon, where you can watch others play games live and listen to commentary as they play. It has 15 million daily active users and more than three million people live broadcast video game streams and other content on Twitch, with channels dedicated to just about every popular video game imaginable—both new and retro. There are also shows that feature gaming competitions, professional tournaments, game-related chat and news. Plus, numerous non-gaming channels covering everything from cookery and music to art and travel. But Twitch is not just about watching other people’s shows—anyone can broadcast their own gaming action.

Top Tips for Parents

**The Risk - It's Live & Uncensored**

As gamers get engrossed in their games, it is very common for their rarer choice words, and the chance of your child encountering swear words and bad language is extremely high. There is not only the language of the person running the stream that you need to consider, but also the language of other Twitch users in the text-based chat that accompanies streams.

**What Parents Can Do**

There’s not much you can do to reduce exposure to bad language on Twitch, but if there are any troublemakers, it is possible to block them. It is a good idea to speak to your child and let them know different channels on the platform, as this will give you an idea of the sort of content they are being exposed to.

As Twitch does not offer any parental control options, this is the best way to police what your child is viewing. If your child is overwhelmed or disturbed by comments that are posted in the stream chat, it is worth hiding it from view by clicking the little arrow to the right of the Subscribe button.

**The Risk - Violent Games & Adult Content**

Like so many apps, Twitch does not allow children under the age of 13 to create an account, but in practice, there is no easy way to stop someone signing up by simply entering a false date of birth. In addition to viewing commentary provided by other Twitch users, you can also contain adult content, and the games themselves can be more violent. But it is important that you check which games are on the market these days have an age rating of 18, and it is indicative of the kind of language, sexual content and violence that they may contain.

**What Parents Can Do**

There is nothing that can be done to prevent your child from accessing violent games. One of the problems with using your router settings or parental control software to block access to the site (as recommended in the guide) is that it is not possible to check which games are on the market these days have an age rating of 18, and it is indicative of the kind of language, sexual content and violence that they may contain.

**The Risk - Unwanted Contact from Other Users**

Just like any website or platform with social elements to it, there is the risk that your child will not only come into contact with the sort of people might rather they didn’t, but also that they could be harassed, groomed or bullied online.

**What Parents Can Do**

Within Twitch settings, in the Security and Privacy sections, you can choose which messages are allowed or blocked, whether strangers can whisper to them, or whether they are allowed to receive messages from anyone who is not approved by you or your child’s friends. Taking things one at a time makes it possible to control their online existence without making them seem overly protective. Show your child how to make use of the options by clicking on their name and in the little pop-up that appears, click the icon that looks like a little speech bubble and check them. If your child wishes to report the user to Twitch, click the three dots button beneath the block option and click report.

**The Risk - Webcam Sharing**

As well as seeing streaming footage of games, Twitch also lets users share the content from their webcam. This gives yet another way for people to share inappropriate content, and it adds another layer to sexualised content from your child to advertise, sponsored content and product placement.

**What Parents Can Do**

Getting involved in your child’s use of Twitch is the best way to keep an eye on the sort of content they are consuming and intervene if anything inappropriate crops up. As part of our conversations with your child about what is appropriate to share online, try to educate them about careful use of their own webcam if they choose to stream their own gaming. As well as ensuring they are not encouraged into doing anything inappropriate on camera, it is also important to check that anything that can be used to identify them is not included in shot.

**The Risk - Twitch Emotes**

Twitch’s interactive feature is littered with emoticons or emotes, which are constantly evolving. Every channel features one of the characters, such as a grass-roots photograph of a game developer known as a "srip". Some of these emoticons can be quite complex and can be used for harassment—defined by targeted insults, dehumanisation, and threats of any nature. If your child finds an emoticon that violates guidelines, they can report it on the "User Report Tool". Channel owners can also use specific emoticons to their Channel "Banned Words List".

**What Parents Can Do**

Chat to your child about how they use Twitch and show an interest in understanding how it works. There are lots of online guides to Twitch, so you can get your child up to speed on what is happening in chat. Twitch’s terms of service state that emoticons should not be used for harassment—defined by targeted insults, dehumanisation, and threats of any nature. If your child finds an emoticon that violates guidelines, they can report it on the "User Report Tool". Channel owners can also use specific emoticons to their Channel "Banned Words List".

SOURCES: [https://www.twitch.tv](https://www.twitch.tv)

National Online Safety

www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061
**What parents need to know about Twitter**

**Twitter Trolls**
A troll is someone who deliberately posts negative or offensive comments online in a bid to provoke an individual for a reaction. Trolling can include bullying, harassment, stalking, revenue mobbing and much more – it is very common on Twitter. The motive may be to get the troll victim to react in a certain way or make people laugh. However, the pragmatics of what post could be much more dangerous, provoking anything from social 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 thoughts and opinions. As a result, you will likely see posts anything they want, despite restrictions. Content that violates the rules, if your child sees any inappropriate content, they must tell the website immediately if they are following their account. Additionally, the adult can use the ‘lock’ feature to lock their profile on the platform so that anyone the user follows or is followed by will not be able to see content without it being unlocked.

**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 start or fake 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 all children need to understand the fake news problem.

**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 users may hijack the hashtag for something inappropriate or dangerous that your child shouldn’t be exposed to. It 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 that can be used by anyone to make concepts or ideas go viral across the internet. However, normalisation of topics including racism, sexism and homophobia may not be appropriate for your children. Be aware of any messages that your children may receive, even if they are not following the user.

**Propaganda, Extremism and Radicalisation**
Social media offers a continuous stream of real-time coverage of extremist activity. Twitter is one of the many platforms that is used by extremists to spread their messages. This includes radicalising vulnerable people, young people and to use a way to communicate with and radicalise them.

**Everyone Has Access**
Twitter has over 335 million monthly active users across all age groups, when one user signs up, tweets can be public by default meaning anyone can view and make comments on public tweets. Your child may be using Twitter as a platform where they can share information about any activity they are involved in, even if they don’t think of it, there’s always a chance that someone can screenshot, retweet 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 anywhere, you can always make their account protected. This means that only people who they explicitly select as ‘followers’ will be able to see their tweets. They should also make sure that they have their location set to ‘off’ so that anyone 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, we strongly suggest blocking and reporting them. Blocking them will prevent them from seeing your child’s tweets and reporting their account will alert Twitter to investigate the profile.

**Tweets & Laws**
From 2016, the CPS were able to exercise new laws that could be used to charge people for using Twitter to commit crimes. This includes ”humiliating” photos when images were shared. They also announced the launch of a task force to combat online crime. In 2018, the Ofcom (the official industry regulator) introduced a code of practice that will help protect your child from online bullying.

**Sensitive Content**
By default, only someone who is following the account will be able to see the sensitive content. If you want to moderate potentially harmful images, you can choose to do so. You can then choose what you want to see by choosing the settings. You will be able to see the tweets through the嗣acks and will be able to see the content. If you are not interested in the content, you can report it. Twitter should then inspect the tweet and decide whether they deem it to be sensitive.

**Mute Hashtags & Phrases**
If you want to filter out any of theله black certain words, hashtags or phrases from your child’s timeline or notifications or a tweet with inappropriate phrases, emojis, etc.,

**Twitter Lists**
Twitter lists allow your child to create other feeds outside the main timeline that may only include certain accounts to filter them to segment followers based on common topics and interests.

**National Online Safety**
A whole school community approach to online safety

www.nationalonlinesafety.com

Email us at help@nationalonlinesafety.com or call us on 0800 358 8061

**Source**
- https://www.twitter.com/security/tweet这让账户不显示文字内容
- https://www.twitter.com/security/tweet这让账户不显示文字内容
- https://www.twitter.com/security/tweet这让账户不显示文字内容
- https://www.twitter.com/security/tweet这让账户不显示文字内容

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.
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.

SPENDING A PREMIUM
You Tube Premium (formerly YouTube Red) is a new paid streaming subscription service in the UK, offering a three-month free trial to tempt viewers into £10 per month plan. This includes the ability to download videos, stream videos with the app in the background, give exclusive access to original content and a separate dedicated streaming 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 have been seen 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 video page. Through this chat 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.

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. Use 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 YouTube history. Videos can also be easily downloaded, so it's important that your child understands the associated dangers before 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 YouTube to share with. To get started, your child can see YouTube Studio which allows learning modules on creating a YouTube channel, however, you should encourage them not to use the real name.

NEW FEATURES
- Stampy
- Vlogger Lewis & Simon
- PewDiePie
- EthanGamer
- Markiplier

DIGITAL WELLBEING
YouTube has launched a tool called 'Time Watched' that allows you to see how long your child has 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.

Top Tips for Parents

OPT FOR A FAMILY PREMIUM PLAN
If you have more than one child, it is worth considering YouTube Family Premium. This option will allow you to share a YouTube paid membership with up to five other family members, aged 11 and older, 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 a social media addict, bear in mind that they may be contacted by the 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 children 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 YouTube's are posting. Often, the games they are playing will contain strong language and violence. A few examples of popular YouTube gamers for young people include:

- Stampy
- Vlogger Lewis & Simon
- PewDiePie
- EthanGamer
- Markiplier

- PopularMMO
- Cupcake23
- Jacksepticeye
- LTChris
- DanTDM

NOS
National Online Safety

NOS
National Online Safety

NOS
National Online Safety

NOS
National Online Safety

NOS
National Online Safety

© National Online Safety Ltd

www.nationalonlinesafety.com

#199.99 a month. It allows you to share a YouTube paid membership with up to five other family members, aged 11 and older, 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 a social media addict, bear in mind that they may be contacted by the 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 children 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 YouTube's are posting. Often, the games they are playing will contain strong language and violence. A few examples of popular YouTube gamers for young people include:

- Stampy
- Vlogger Lewis & Simon
- PewDiePie
- EthanGamer
- Markiplier

- PopularMMO
- Cupcake23
- Jacksepticeye
- LTChris
- DanTDM
Yubo is a location-based social networking app previously known as 'Yellow'. It has been dubbed 'Tinder for teens' due to its similarities with the adult dating app, in which users swipe to find matches. Yubo allows users to livestream themselves to anyone watching, and rate other users.

**What parents need to know about Yubo (Formerly 'Yellow')**

**WHO IS USING YUBO?**
Although its official guidelines suggest the app is for people aged 18+, those aged between 13 and 17 can create a profile with parental permission. Furthermore, the app does not verify ages or identities upon sign-up, leading to fears that it could be exploited by those seeking to target children. Adults can set up fake profiles for sexual reasons, while children younger than 13, with access to the Internet, could pretend to be older than they are.

**LIVE-STREAM FOOTAGE**
Yubo states that it uses a combination of technical tools and human moderators to check the content created by Yubo. But since users can comment on footage in real-time, this could mean that children could be exposed to derogatory or unpleasant language. Media reports indicate that teens are being pressured into undressing live on camera for strangers, sending nude photos, and are even lured into face-to-face meetings on Yubo. Any users can take screenshots or copies of live streams, alter them and share them with others.

**SNAPCHAT**
While the Yubo app doesn’t directly link to Snapchat anymore – users still tend to share their Snapchat usernames on their profiles, making them very easy to add on Snapchat without ever speaking to the individual. On Snapchat, if your child’s location feature is switched on, there is a high chance that strangers can find your child’s exact location.

**BULLYING & MENTAL HEALTH**
The way Yubo works is that users ‘swipe’ to accept or decline to talk to someone. Whether users accept or decline is all based on their profile picture, meaning there is the potential that children could be left with low self-esteem if declined. Receiving comments about their appearance can have a negative impact on a child’s emotional wellbeing, leaving them feeling less confident about how they look or how interesting they are. Bullying includes actions or comments that are intended to cause harm, but spreading false rumour about people. As users have the ability to screenshot copies of live streams and private messages etc., they can use these screen grabs as forms of blackmail, making the person feel victimised, embarrassed and unsafe.

**Top Tips for Parents**

**HAVE A CHAT**
Start a conversation with your teenager so that they know how to stay safe online. Don't be embarrassed to talk about inappropriate online content with your children and look out for secretive or reserved behaviour when it comes to their Internet devices.

**DISCUSS YUBO GUIDELINES**
Take time to go through Yubo’s Community Guidelines, which all users receive a link to, when they sign up to the app. Anyone who does not follow the guidelines may have their account suspended. Guidelines include advice on not posting any fake pictures or pretending to be anyone else.

**YUBO GUIDELINES FOR PARENTS**
Yubo offers a guide to parents, which outlines its ‘five-step approach to safety’, including: Sign-up, Profile Settings, Community Guidelines, Moderation and Reporting.

**REMOVE LOCATION FEATURE**
In their ‘Profile’ settings, children can hide their city and choose to connect with people who are only located within a certain radius of their location.

**PROOF OF AGE**
Yubo recently updated its security settings so that users who attempt to change their date of birth after signing up have to send proof of ID to the app in order to verify the change.

**ENCOURAGE RESPECT**
Remind your teenager to always consider anything they are about to share online and to think about whether they would do that in the ‘real world’, or whether they are posting something they may regret at a later date.

**AVOIDING UNEXPECTED IMAGES**
Yubo suggests that teenagers ask the people they are talking with to share a picture of themselves with a spoon on their head to prove they are really who they say they are in their picture. Another tip is to avoid profiles with only one photo as these are often ‘Cafish’, someone who pretends to be somebody else by creating false identities.

**PREPARE FOR ‘GOING LIVE’**
Yubo users can ‘Go Live’ during a chat with friends or choose to live stream ‘Anyone’ on Yubo. To help your child avoid sharing too much, help them to consider whether they really want the world seeing what they are doing. If they are going to watch streams they should also know how to report anything that makes them feel upset, uncomfortable.

---

**National Online Safety**
A whole school community approach to online safety

[www.nationalonlinesafety.com](http://www.nationalonlinesafety.com)

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

---

What parents need to know about WhatsApp

AGE LIMIT CHANGE
Since May 2018, the minimum age for using WhatsApp is 16 years old. If you live in the European Union, children under 16 are not allowed to use WhatsApp. Prior to this, the minimum age was 13, which still applies for the rest of the world. WhatsApp has not yet stated whether it will take action against anyone aged between 13 and 16 who already hold accounts under the old terms and conditions, such as closing their account or asking for parental permission.

SCAM MESSAGES
Occasionally on WhatsApp, people receive spam messages from unauthorised third parties or from fraudsters pretending to offer prizes to 'lucky' people, encouraging recipients to click on a link to win a prize. A common scam involves message warning recipients that their WhatsApp subscription has run out with the hope that people are duped into providing their payment details. Other scam messages include instructions to forward the message in return for a reward or gift from WhatsApp or another person.

FAKE NEWS AND HOAXES
WhatsApp has been linked to enabling the spread of dangerous viral rumours. In India, for example, a number of attacks appear to have been sparked by false rumours shared on WhatsApp.

THE 'ONLY ADMIN' FEATURE AND CYBERBULLYING
Cyberbullying is the act of sending threatening or taunting text messages, voice messages, pictures and videos, with the aim to hurt and humiliate the receiver. The 'only admin' feature on WhatsApp allows the admin of a group chat to block video call features for specific people. However, this can be used by the admin for one-way announcements, the group has the power to block somebody from responding to an offensive message in a chat, which could result in a child being upset and unable to reply.

CONNECTING WITH STRANGERS
To start a chat in WhatsApp, you need to know the mobile number of the contact you want to speak to and they also need to have the app downloaded. WhatsApp can find contacts by accessing the address book of a device and recognising which of those contacts are using WhatsApp. If your child has shared their mobile number with someone they don’t know, they can use it to get in touch via WhatsApp.

LIVE LOCATION SHARING
WhatsApp’s ‘Live Location’ feature allows users to share their current location in real time to their contacts in a chat, allowing friends to know their movements. The feature can be found by pressing the ‘attach’ button. It is described by WhatsApp as a “simple and secure way to let people know where you are”. Location sharing is already a common feature on other social apps, including Snapchat’s Snap Map and Facebook Messenger, and can be a useful way to a child to let loved ones know they are safe. However, if your child is in a group chat with people they do not know, they will be exposing their location.

CREATE A SAFE PROFILE
Even though somebody would need your child’s phone number to add them as a contact, it is an extra security measure we suggest altering their profile settings to control who can see their profile picture. The options to choose from are ‘Everyone’, ‘My Contacts’ and ‘Nobody’. We suggest selecting ‘My Contacts’ or ‘Nobody’ to ensure their profile is protected.

EXPLAIN HOW TO BLOCK PEOPLE
If your child has received spam or offensive messages, calls or attachments from a contact, they should block them. Messages and status updates sent by a blocked contact will not show up on the phone and will stay undelivered. Blocking someone will not remove this contact from the contact list, they will need to be removed from the phone’s address book. To block a contact, your child needs to open the person’s chat streams and tap on the settings.

REPORT SCAM MESSAGES
Advise your child not to tap or forward any message that looks suspicious or sounds too good to be true. When your child receives a message from an unknown number for the first time, they will be given the option to report the number as spam directly inside the chat. They can also report a contact or a group as spam in the following steps: 1) Open the chat, 2) Tap on the contact or group name to open their profile information, 3) Scroll to the bottom and tap ‘Report Spam’.

DELETE ACCIDENTAL MESSAGES
If your child has sent a message to the wrong chat or if a message they sent has contained a mistake, they can delete it. To do this, simply tap and hold on the message, choose ‘Delete’ and then ‘Delete for Everyone’. The app allows seven minutes to delete the message after it has been sent, but it is important to remember that recipients may have seen and screenshot a message before it was deleted.

SET TIME LIMITS
A 2017 study found that by the age of 14 the average child will have sent more than 37,500 texts. 36,000 WhatsApp messages and racked up more than three solid weeks of video chat. Although it is inevitable that your child will use technology, you can still set boundaries. This is not easy, especially since teenagers use their devices for both schoolwork and free time, often simultaneously.

© National Online Safety Ltd
This is not a prescriptive guide. Please always check with the app’s support information to see if your languages and priorities coincide and expand.
What parents need to know

LiveMe is a streaming video app that lets you watch live streams and broadcast your own live videos to anyone interested. The service, which claims to have over 60 million global users and streams around 300,000 hours of footage a day, is aimed at giving creators a "platform to reach a wide audience and share their talents and passions directly with their fans." Users can buy virtual coins and gifts and send these to broadcasters who create content "they love, which can be redeemed for real money.

**ONLINE PREDATORS**

Law enforcement agencies have warned that LiveMe is placing children at risk from online predators. A sheriff in Texas even issued a memo that predators have a virtual open window to your child's bedroom. Live that can be accessed by anyone to target your child who may be sharing personal information and engaging with sexual images and videos. LiveMe also has a "chat feature," which allows users to speak to each other in private. In 2018, a 65-year-old in the UK was jailed for posing as a teenage boy to get into a room on LiveMe and offered virtual currency to exchange for teenagers exposing themselves.

**INAPPROPRIATE & ADULT CONTENT**

Live streaming apps can potentially expose young people to graphic and inappropriate content. LiveMe says it is "explicitly intended to be used by individuals 17 years of age or older." If you have concerns, you should ask your child if they would be comfortable sharing their personal information and thoughts with someone else.

**SPENDING MONEY ON VIRTUAL GIFTS**

Coins are the LiveMe currency. Viewers and broadcasters can buy coins and use them to purchase gifts or coins to drop on chat with another. When viewers send gifts, they immediately earn the same number of diamonds. Once someone has made a certain level of diamonds, they can cash them out for real money or convert them back into coins. There is always the danger of children spending too much on in-app purchases without knowing.

**BROADCASTING TO STRANGERS**

It is important for children to understand the risks of broadcasting and live streaming services have limited privacy controls, so it is hard to know who is watching and is difficult to prevent people accessing the stream. Explain to your child that it is possible for any video to be recorded and shared without the permission or knowledge of the person who made the video.

**REPORT INAPPROPRIATE BEHAVIOUR**

If someone has been acting inappropriately, you are encouraged to ask for help by emailing LiveMe/ccmc.com with the subject line:"ATTENTION: INAPPROPRIATE BEHAVIOUR" and send evidence, including a screenshot of their profile. You can also directly report inappropriate, offensive, and harmful content from inside the app using the Report option. However, it is worth remembering that it is not wise to screenshot and save inappropriate material.

**BLOCKING PEOPLE**

Explain to your child that if they notice inappropriate behavior, bullying, or any other rule-breaking conduct on LiveMe, they can block a user from chatting on their broadcast and profile by tapping on their name, navigating to the profile page, and then choosing ‘block’.

**RESTRICT IN-APP PURCHASES**

Stop your children from making in-app purchases by changing the app and device settings. For example, you can change the settings to prevent an individual with a password is required to proceed with a transaction. Advise your child not to buy anything online without talking to you first.

**LOCATION SHARING**

Publishing live videos that list your child's location or identity is dangerous. People will be able to use this information. Explain to your child that they need to think carefully about where and when they broadcast live.

**THINK BEFORE YOU BROADCAST**

As with anything that is posted and shared with other people and online, remember that once it is up, it is hard to take back. Images and videos can come back to haunt your child, often by street names or school uniforms. Explain to your child that they need to think carefully about where and when they broadcast live.

**BE RESPECTFUL OF OTHERS**

Remind your child to always consider what they are about to comment on and to think about whether they would do the same if they were being commented on by someone else.

**DISCUSS SEXTING**

Although it is an awkward subject, it is important to explain to children that creating or sharing explicit images of a child is illegal. If your child is posting images of themselves or others, encourage them to think about the language they use, online and to think carefully before commenting on content posted by someone else.

**Top Tips for Parents**

- Educate your child about the risks of broadcasting and live streaming services.
- Encourage your child to use the built-in privacy features.
- Monitor your child's use of the app to ensure they are not sharing personal information.
- Install content filters to prevent inappropriate content from being viewed.
- Set age restrictions and block inappropriate content.
- Encourage your child to report any inappropriate behavior they encounter.
- Discuss the implications of sexting and the importance of keeping their content private.

**Sources**


**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
What parents need to know about GRAND THEFT AUTO (GTA)

Top Tips for Parents

**The Risk - Playing with Strangers**

When buying GTA V you automatically have access to Grand Theft Auto Online, a version of the game that allows players to play online. They can play alone, invite players to games, or be involved in minigame 'sessions' where people will be picked at random to play. When you first load into a game you are automatically placed into an open lobby, meaning you play with random people. The social club is GTA's own social platform where users can bet money, share in-game photographs (which users can like and comment on), and even message other users directly.

**What parents can do**

To prevent your child playing with strangers on the game, you can change the settings to ensure they only play with their friends and nothing else. Upon signing up to the 'social club', it automatically sets a player's visibility settings, which means that their name and profile information is made public. Parents can alter this by changing the visibility settings to 'only me'.

**The Risk - Addiction**

Addiction is a risk with any game. Game developers use persuasive design techniques to force users to invest their time, and often money, in a game. Within GTA, your character is able to progress through the game for completing missions within a certain time frame, encouraging children to keep returning to the game. Gaming addiction is a recognised health condition and the side effects are concerning including sleep deprivation, decreased attention span and erratic emotional behaviour.

**What parents can do**

There are a number of things you can do if you are concerned about your child's screen time, including setting time limits within the home, especially during meal times and before bedtime. Talk to your child and ask why they are spending so much time on the game, and encourage healthier alternatives such as outdoor activities and spending quality time with friends and family.

**The Risk - Live Chat**

When playing GTA online, players have the option to use a microphone to broadcast their voice live to other players involved in the 'session'. These live voice chats are not moderated, meaning anything could be said, including inappropriate language, as well as verbal forms of bullying.

**What parents can do**

Talk openly with your child about not giving away personal information. Also remind them that conversations can be recorded, which could damage their online reputation. Depending on the device/platform, there will be ways to mute conversations. Make yourself aware of the device/platform's individual settings and ensure that your child knows how to block and report.

**The Risk - Online Hackers**

Hackers can make money by helping users cheat in the game. They can do a number of inappropriate things, including killing people, stealing weapons, spawning money into the game, and even raping other characters. Spawning money tends to be a game's most popular choice, being able to buy $100,000,000,000 in-game currency for as little as five US dollars.

**What parents can do**

Actively monitor your child's online activity. These websites are very easy to find, meaning children and young people can easily navigate their way to these websites and pay for hacks. Hackers tend to engage in illegal activity, but you have the risk of giving your personal information to someone who may misuse it.

**The Risk - Microtransactions**

By completing missions and partaking in certain activities you earn in-game currency. This allows you to buy things such as prostitutes, vehicles, weapons, ammo, new outfits, cars, apartments and more. However, the items that are available to buy often have a high price that require a lot of game time, meaning the items are effectively unrealistic to buy.

**What parents can do**

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 purchasing a pre-paid gift card for your child. These can be purchased in specific amounts which will allow you to limit how much your child spends and remove the need for a credit or debit card to be used with their account.

Sources:

- https://www.imdb.com/title/tt12163188/parentalguide
- https://www.telegraph.co.uk/gaming/news/grand-theft-auto-v-has-made-money-film-history/

---

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
Momo is a sinister challenge that has been around for some time. It has recently resurfaced and once again has come to the attention of schools and children across the country. Dubbed the ‘sUicide Killer game’, Momo has been heavily linked with apps such as Facebook, WhatsApp, YouTube, and most recently (and most worryingly)... YouTube Kids. The scary doll-like figure reportedly sends graphic violent images, and asks users to partake in dangerous challenges like waking up at random hours and has even been associated with self-harm. It has been reported that the Momo figure was originally created as a sculpture and featured in an art gallery in Tokyo and unrelated to the Momo challenge we are hearing about in the media.

What parents need to know about Momo

**Children's Videos Being 'Hijacked'**

There have been recent reports that some seemingly innocent videos on YouTube and YouTube Kids (such as ‘surprise eggs’, unboxing videos and Minecraft videos) have been edited by unknown sources to include violence provoking and/or other inappropriate content. Even though YouTube monitor and remove videos that include inappropriate content, clips can be uploaded and viewed thousands of times before they get reported and removed. As a parent, it’s difficult to spot these videos as the harmful content doesn’t appear until partway through the video.

**Distressing for Children**

Popular YouTubers and other accounts have been uploading reaction videos, showing their experience of the MOMO challenge. Sometimes the video includes a disclosure message warning that the content may be “inappropriate or offensive to some audiences” and that “viewer discretion is advised” but these videos are still easily accessed by clicking ‘understand’ and wish to proceed. The image of the MOMO character can be deeply distressing to children and young people and it’s important to note that it may slip through parental settings and filters.

**Suggested Videos on YouTube**

Video apps such as YouTube include an ‘up next’ feature which automatically plays another video based on the video just watched. Due to YouTube’s algorithm, users are shown ‘suggested videos’ that they may be interested in. The thumbnails used on suggested videos are purposefully created in a way to encourage viewers to click them. During our research, we found that when watching one Momo related video, we were shown countless other Momo themed videos and other scary content which would be age-inappropriate for children under 18.

**National Online Safety**

Tell Them It’s Not Real

Just like any urban legend or horror story, the concept can be quite frightening and distressing for young people. Whilst this may seem obvious, it’s important for you to reassure to your child that Momo is not a real person and cannot directly harm them. Also, tell your child not to go openly searching for this content online as it may cause more distress.

Be Present

It’s important for you, as a parent or carer, to be present while your children are online. This will give you a greater understanding of what they are doing on their devices as well as providing you with the opportunity to discuss, support and stop certain activities that your child may be involved in. As the nature of each task becomes progressively worse it’s also important to recognise any changes in your child’s behaviour.

Talk Regularly With Your Child

As well as monitoring your child’s activity, it’s important for you to discuss it with them too. Not only will this give you an understanding of their online actions, but these honest and open conversations will encourage your child to feel confident to discuss issues and concerns they may have related to the online world.

**Device Settings & Parental Controls**

Ensure that you set up parental controls for your devices at home. This will help to restrict the types of content that your child can view, as well as help you to monitor their activity. In addition to this, it’s vital that you are aware of your device and account settings to ensure your child’s utmost safety. For example, on YouTube you can turn off ‘suggested auto-play’ on videos to stop your child from viewing content that they have not directly selected.

**Peer Pressure**

Trends and viral challenges can be tempting for children to take part in no matter how dangerous or scary they seem. Make sure you talk to your child about how they shouldn’t succumb to peer pressure and do anything they are not comfortable with, online or offline. If they are unsure, encourage them to talk to you or another trusted adult.

**Real or Hoax?**

As a parent it is natural to feel worried about certain things you see online that may be harmful to your child. However, not everything you see online is true. Check backgrounds and be mindful of what you share as it may only cause more worry.

**Top Tips for Parents**

**Report & Block**

You can’t always rely on parental controls to block distressing or harmful material. People find their way around a platform’s algorithm in order to share and promote this type of material. Due to this, we advise that you flag and report any material you deem to be inappropriate or harmful as soon as you come across it. You should also block the account/content to prevent your child from viewing it. Also encourage your child to record a screenshot of any content they feel could be malicious to provide evidence in order to escalate the issue to the appropriate channels.

**Further Support**

Speak to the safeguarding lead within your child’s school should you have any concerns regarding your child’s online activity or malicious content that could affect them.

If your child sees something distressing, it is important that they know where to go to seek help and who their trusted adults are. They could also contact Childline where a trained councillor will listen to anything that’s worrying them.

The Childline phone number is 0800 1111.