



BARKING ABBEY SCHOOL

ONLINE SAFETY GUIDE

BELONG
BARKING

ASPIRE
ABBAY

SUCCEED
SCHOOL

www.barkingabbeyschool.co.uk

SOCIAL MEDIA & Mental Health

What trusted adults need to know

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

Five potential signs & symptoms of mental health difficulties

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

NOS National Online Safety®
#WakeUpWednesday

Meet our expert

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



1. EDUCATE YOURSELF

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

2. DISCUSS REAL-LIFE CONNECTIONS

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



3. SUGGEST REGULAR BREAKS FROM SOCIAL MEDIA

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



4. ENCOURAGE OTHER HOBBIES OR INTERESTS

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



5. OFFER YOUR SUPPORT

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

HELPFUL APPS:

- Hub of Hope
- Mindshift
- Smiling Mind

OTHER SERVICES:

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

Sources: <https://www.centreformentalhealth.org.uk/publications/social-media-young-people-and-mental-health>, <https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/articles/measuringnationalwellbeing/2015-10-20>, <https://www.rspg.org.uk/uploads/assets/uploaded/62be270a-a55f-4719-ad668c2ec7a74c2a.pdf>, <https://www.psychologytoday.com/us/blog/cutting-edge-leadership/201505/5-warning-signs-mental-health-risk>

WHAT TRUSTED ADULTS NEED TO KNOW ABOUT: SOCIAL MEDIA & MENTAL HEALTH

Social Media is often scrutinised as having a negative impact on children's mental health. Children and young people are now growing up in a technology dominated world, and social media plays a major role in their social lives. This balanced guide focuses on both the positive and negative impacts that social media can bring to young people and their mental health.

POSITIVE IMPACTS

EASY ACCESS TO SUPPORT AND HELP

Due to delays in young people getting help for their mental health, such as experiencing low mood, or suffering from anxiety, they may sometimes reach out to access support from others online. Sharing problems or issues with friends, peers and broader social networks can be met with positive reaction, with nearly 7 in 10 teens reporting to receive support on social media during tough or challenging times. Where there are moderated communities which offer support and guidance, children can be provided with a great source of support.

SUSTAINING FRIENDSHIPS AND MAKING CONNECTIONS

There is evidence to suggest that strong adolescent friendships can be enhanced by social media interaction, allowing children to create stronger bonds with people they already know. Online relationships can actually make children more relationship-oriented, thoughtful, and empathic. By sharing comments on pictures, videos and posts, it can create long-term friendships as they can continually keep in touch, even with a distance between them.

A SENSE OF BELONGING

Support can be found in various places online; sometimes this is known as "finding your tribe". Online platforms and groups can provide a wonderful sense of belonging for children. They can find peers with similar interests and circumstances which can sometimes be difficult to find in real-life. As a result, this can create stronger connections and help to build confidence.

NEGATIVE IMPACTS

SELF-ESTEEM & BODY IMAGE

There are 10 million new photographs uploaded to Facebook alone every hour, providing an almost endless potential for young people to be drawn into appearance-based comparisons whilst online. No one is the same as how they portray themselves online as we tend to only show the best part of ourselves. The pressure to fit-in and conform is huge, which can become a driving force for children to replicate what they see from friends, celebrities and sponsored adverts. This pressure may contribute to anxiety, low mood and a feeling of inadequacy. As a result, it can lead to a feeling of low satisfaction with their own lives.

HARMFUL ADVICE

The online world provides the opportunity for anybody to upload and share photoshopped pictures, edited video, fake news and even unvetted advice. Children may stumble upon this, which could potentially encourage them make wrong decisions and not get the help that they need. It's important that you teach your child to differentiate between what is true and useful information and what is fake.

ADDICTION AND COMPULSIVE CHECKING

Social media addiction is thought to affect around 5% of teenagers. The Office for National Statistics found that children who spend more than 3 hours a day on social media are more than twice as likely to support poor mental health. Furthermore, compulsive checking due to 'Fear Of Missing Out' has been linked to poor and disturbed sleep, as well as difficulty to relax during evenings. One in five young people say they wake up during the night to check messages on social media, leading them to be three times as more likely to feel constantly tired at school than their classmates who don't use social media during the night.

CYBERBULLYING

One recent large-scale UK study showed that cyberbullying is one of the biggest challenges for young people. Other studies suggest that cyberbullying has a bigger effect on wellbeing and mental health than other types of bullying, 7 in 10 young people have experienced cyberbullying, with 37% of young people saying they experience cyberbullying on a high-frequency basis. Young people are twice as likely to be bullied on Facebook than on any other social network.



- Hub of Hope - <https://hubofhope.co.uk/>
- Mindshift
- Smiling Mind

- Childline, 0800 1111 or visit their website
- Bullying UK, 0808 8002222
- Young Minds Parents line, 0808 802 5544

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

1 PUT YOURSELF IN CONTROL

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



2



PROTECTING ANDROID DEVICES

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

3 PROTECTING APPLE DEVICES

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



4

THINK ABOUT ALL YOUR SMART DEVICES

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



5



MAKE SEARCHING MUCH SAFER

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



9 Top Tips To Get Smart About children's devices

6

REGULARLY CHECK SOCIAL MEDIA SETTINGS

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



7



DON'T LET PEOPLE SEE WHERE YOU ARE

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

8 WATCH OUT FOR FAKE PROFILES

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



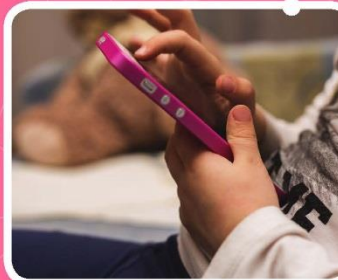
9 KEEP A CHECK ON SCREEN TIME

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



Meet our expert

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



Smart devices promise to make our lives easier. In many cases - they do, however these new technologies present risks too. Whether you're using a digital assistant to record your shopping list or you're controlling your lights through a smart system, many smart functions can be 'hacked' and controlled by someone outside your home. This guide will help you identify some of the ways you can stay alert and protect yourself.


1 KNOW THE RISKS

The success of any smart device relies on it communicating with other devices using the Internet. It's an unavoidable part of using smart devices, but it does expose you to numerous risks. Attackers could use the Internet connection to steal your data for identify fraud or to make unauthorised purchases through your devices. There is even potential for more sinister exploitation, such as child grooming or cyber-bullying.




2 WHAT IS THE INTERNET OF THINGS?

This is the term given to all the devices connected to the Internet in your home. It includes a new digital doorbell connected to your smartphone, your kettle that boils when you tell it to on your tablet or your heating that comes on when you swipe on your smart watch. The Internet of Things (IoT) is designed to make life easier, but it also opens up your home network to potential cyber-attacks. It doesn't mean you can't enjoy the benefits, but it does mean being aware of the potential negatives.



3 CHECK ENCRYPTION SETTINGS

Whenever data is sent over the Internet, it is 'encrypted'. This makes it harder to read if it's intercepted. You should look to use a strong encryption setting, such as WPA2, rather than WPA or WEP. You can check your router manual on how to do this.


4 KEEP YOUR SOFTWARE UP TO DATE

Manufacturers constantly update and improve software used in smart devices. Some will automatically alert you to an update, but not all do. To be on the safe side, it's a good idea to set reminders in your calendar. Check the manufacturer's website for any updates and run them if necessary.



5 RENAME THE 'GATEWAY' TO YOUR HOME

Your Internet router is the virtual gateway to your home network. It needs protecting. To do this, you should change the default name (the SSID) and password. You can usually find steps to do this in the instruction manual. Don't use your family name. Choose something more obscure. Make the password complicated too, using upper and lower-case letters, numbers and symbols. Do this for your router and any other smart devices connected to the Internet.



12 Top Tips To Get Smart About The DEVICES In Your Home

NOS National Online Safety®




6 USE A SEPARATE NETWORK FOR GUESTS

If your router has a feature that allows you to set up a separate network for guests, you should use it. That way, when guests use your Wi-Fi, they won't have access to your devices.

9 TRUST YOUR INSTINCTS

If you ever feel something is wrong or your network is being exploited, visit the manufacturer's website or ring their technical support department. It's better to be safe than sorry.



7 SAY GOODBYE TO SIRI AND ALEXA

It's a good idea to change the activation words on your smart devices so they are unique to you and your family. This makes it that much harder for people to break into your smart devices.



8 DEACTIVATE ANY UNNECESSARY FEATURES

Though it's a fun idea, you probably don't need to control your kettle from outside the house. In fact, there are often many unnecessary features included on smart devices. Where possible, you should look to disable these. Doing so reduces the ability for people to hack your devices. When someone sees you've actively taken steps to increase security, they're less inclined to try to compromise them.



10 BUILD A WALL

You could also purchase a dedicated 'firewall' device. This is something that plugs into your network and stops cyber threats reaching your router. Some routers do have a firewall element included, but they are no replacement for the real thing. A firewall device thoroughly analyses information coming in and out of your network and helps stop malicious attacks. A security device is strongly recommended to anyone who works from home or deals with sensitive information.



11 SECURE YOUR SMARTPHONE

If you do use apps on your smartphone to control devices in your home, make sure your smartphone is secure. At the very least makes sure the pin function is enabled, as well as any biometric authentication you have. Where possible, it's also a good idea to download some anti-virus software for your smartphone too.



Meet our expert

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




12 REGULARLY AUDIT YOUR DEVICES AND CONSOLES

Every now and then you should check through all of your smart devices (including games consoles connected to the Internet). Turn them off at the mains and disconnect them from the Internet. In fact, it's good practice to disconnect any devices that aren't in use. It's a small thing but really does help. Even when you think a device might be in sleep mode, if it's connected to the Internet it could still be listening or streaming data.



SOURCES: <https://www.ncsc.gov.uk>, <https://www.getsafeonline.org>



National Online Safety

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

#WakeUpWednesday

Publish date: 07/11/18



1



Which apps/games are you using at the moment?

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

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.



2

3

PLAY AGAIN?
YES NO

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.



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.



4

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.



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.



6

7

Do you know your limits?

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



What children need to know about

ONLINE BULLYING



What is online bullying?

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

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

BE KIND ONLINE

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

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



National
Online
Safety

#WakeUpWednesday



Why does it happen?

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

How does it feel to be bullied?

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



Am I an online bully?

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



Who do I tell?

YOU DON'T HAVE TO DEAL WITH THE BULLYING ON YOUR OWN. TALK TO AN ADULT THAT YOU TRUST – A PARENT, GUARDIAN, OR TEACHER. MOST WEBSITES, SOCIAL MEDIA WEBSITES AND ONLINE GAMES OR MOBILE APPS LET YOU REPORT AND BLOCK PEOPLE WHO ARE BOTHERING YOU. YOU COULD ALSO CONTACT CHIDLIN (WWW.CHIDLIN.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.



Publish date: 06/02/19



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:

Universal, suitable for all ages	Parental Guidance required	Suitable for people aged 12 and over	Suitable for people aged 12 and over, anyone younger must be accompanied by an adult
Suitable for people aged 15 and over	Suitable for people aged 18 and over	Adult content only available in specially licenced cinemas and specialist retailers	

WHAT ELSE CAN BBFC REVEAL?

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.

Source: www.bbfc.co.uk

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.

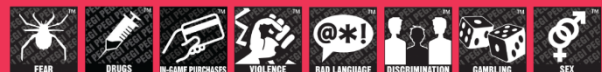
WHAT ARE THE PEGI RATINGS?

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:

www.pegi.info	www.pegi.info	www.pegi.info	www.pegi.info	www.pegi.info

PEGI content descriptors are broken down into eight categories:



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.pegi.info



AGE RESTRICTION
12+



FORTNITE BATTLE ROYALE

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



What parents need to know about FORTNITE: BATTLE ROYALE

MICROTRANSACTIONS

Newly featured items are released daily and are only available to purchase within 24 hours of their release. These are cosmetic items, called 'skins' 'gliders' and 'emotes', which change the characters' appearance, but do not improve the game play. Once purchased, the player has full use of these in the future. The designs are attractive for players to purchase and even celebrities are endorsing them. Also available to purchase in the game is a 'Battle Pass.' When a new 'Battle Pass' is released, users can take part in a series of challenges, receiving more rewards (cosmetics) 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 "dozens" of online reports from people who said their accounts had been compromised by hackers, who had gained access to user's accounts in the game and accrued hundreds of pounds in fraudulent charges.

NO PROOF OF AGE REQUIRED

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

IT CAN BE ADDICTIVE

Games can last around 20 minutes but this varies according to the game. Children may feel angry if 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 for them to stop playing halfway through as their position in the game could be affected.

TALKING TO STRANGERS DURING SQUAD MODE

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

TALKING TO STRANGERS DURING SQUAD MODE

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

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 whilst in the classroom. As the game is available outside of the home, parents may not be aware of how long their child is playing this game.

'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.

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

Top Tips for Parents

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 will soon be available on all mobiles. With this in mind, it is worth having a conversation with your child to discuss and agree how long you would like them to play the games for. Even though the games last around 20 minutes, it may be difficult to take them away from a game mid play. It may be worth imposing a limit on the amount of matches they play rather than a time limit.

LOOK OUT FOR VBUCK SCAMS

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

SHOW THEM HOW TO MAKE A REPORT

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

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 anybody, including their friends. However, they would still be able to use the in-app chat and hear other people's conversations. To turn off voice chat, open the Settings menu in the top right of the main Fortnite page, then click on the cog icon. Open the Audio tab at the top of the screen. From there, you can turn off voice chat.

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, we suggest using a paysafecard, or a games console gift card. 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/debit card to be used with their account.

USE A STRONG PASSWORD

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



**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

<https://www.microsoft.com/en-gb/store/p/fortnite-deluxe-founders-pack> <http://www.bbc.co.uk/news/newsbeat-43626075>
<http://fortnitehelp.epicgames.com/> <https://pegi.info/> <https://www.forbes.com/sites/eriklain/2018/03/12/fortnite-take-hacked-how-to-protect-yourself-and-what-to-do-if-youve-been-compromised/#140c3e7ca719>

Edit date: 29/05/19



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



What parents need to know about SNAPCHAT



EXPOSING YOUR CHILD'S EXACT LOCATION

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

ADDICTIVE SNAPSTREAKS

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

SEXTING

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

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



EXTRAS TO MAKE YOU STAY

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

DAMAGE TO CONFIDENCE

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



Top Tips for Parents



THE RISKS OF SEXTING

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

REPORTING A STORY, LENS, FILTER, SNAP OR MESSAGE

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



USE 'GHOST MODE'

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

HOW TO DELETE A MESSAGE

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

TURN OFF 'QUICK ADD'

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

RESTRICT STORY VIEWS

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



FIFA 19



You don't need to be the biggest football fan in the world to have heard of FIFA (Fédération Internationale de Football Association) - the governing body for football. And, the video game series bearing the organisation's name is one of the most successful ever. The lure of this football series is that official licensing gives your child the opportunity to play games in the role of their favourite players. They can either work through a story mode version of the game or play online in competitions against other players. The game, released annually by Electronic Arts under the EA Sports label, is available for a range of consoles, and there are also mobile versions available for smartphones and tablets. The most recent version is FIFA 18, but FIFA 19 is due for release later in the year.



What parents need to know about **FIFA**

CONSTANT SERIES REFRESHES

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

*** # " @ \$**
IN-GAME CHAT * # " @ \$

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

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

JUST ONE MORE GAME

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

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

Top Tips for Parents



CONSTANT SERIES REFRESHES / WHAT TO DO?

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

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

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

BUYING ADD ONS

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

JUST ONE MORE GAME

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

FIFA GAMEPLAY

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

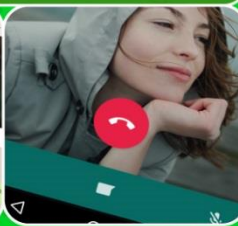
SOURCES
<http://press.ea.com/products/p1532/ea-sports-fifa-18>
<https://www.telegraph.co.uk/men/relationships/fatherhood/10886939/My-son-spend-hundreds-of-pounds-on-in-app-purchases-without-me-knowing.html>
<https://help.ea.com/en-gb/help/fifa/be-safe-with-fut-coins-and-ffa-points/>



WhatsApp is one of the most popular messaging apps in the world, with more than 1.5 billion people in more than 180 countries using it to send and receive text, photos, videos and documents, as well as make voice and video calls through an Internet or Wi-Fi connection. The free app offers end-to-end encryption, which means that messages can only be read by the sender and the recipient in one-to-one chats, or all members if it is a group chat. Not even WhatsApp can read them.



AGE RESTRICTION
16+



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, including the UK. 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 seeking 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 messages 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 group chat and group video call features are great for multiple people to chat simultaneously, but there is the potential for people to hurt others with their comments or jokes. The 'only admin' feature gives the admin of a group chat greater control over who can send messages. Whilst this can be good for one-way announcements, the group admin 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 some-body they don't know, they can use it to get in touch via WhatsApp.

LIVE LOCATION SHARING
WhatsApp's 'Live Location' feature enables users to share their current location in real time to their contacts in a chat, allowing friends to show their movements. The feature, which can be found by pressing the 'attach' button, 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 for 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.



Top Tips for Parents



CREATE A SAFE PROFILE
Even though somebody would need your child's phone number to add them as a contact, as an extra security measure we suggest altering their profile settings to control who can see their profile photo and status. 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 stream and tap on the settings.

REPORT SCAM MESSAGES
Advise your child not to tap, share 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 using 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.'

LEAVE A GROUP
If your child is part of a group chat that makes them feel uncomfortable or has been added to a group they don't want to be part of, use the group's settings to show them how to leave. If someone exits a group, the admin can add them back in once, if they leave again, they cannot be added again.

USING LIVE LOCATION SAFELY
If your child needs to use the 'Live Location' feature to share with you or a friend, advise them to only share it for the amount of time they need to. WhatsApp gives the options of either 15 minutes, one hour or eight hours. However, your child can choose to stop sharing at any time.

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 35,000 texts, 30,000 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 teens use their devices for both schoolwork and free time, often simultaneously.



SOURCES: <https://www.theguardian.com/technology/2018/apr/26/whatsapp-plans-to-ban-under-16s-the-mystery-is-how>; <https://whatsappbrand.com/>; <https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-update-latest-india-hoaxes-forward-messages-app-download-a8456011.html>



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



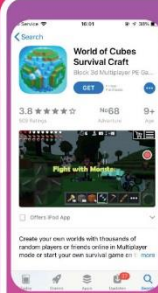
What parents need to know about THE APP STORE

IS YOUR CHILD 13+?

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

IN-APP PURCHASES

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



LOOKALIKE APPS

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

INAPPROPRIATE APPS

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

THIRD-PARTY APP STORES

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



Top Tips for Parents

CREATE YOUR CHILD'S ACCOUNT

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

SWITCH ON 'ASK TO BUY'

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

RESTRICT IN-APP PURCHASES

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

BROWSE APPS BY AGE

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

AVOID OTHER APP STORES

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

HOW TO KNOW AN APP IS SAFE TO INSTALL

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

SPOT FAKE REVIEWS

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

SOURCES: <https://www.engadget.com/2017/12/18/fake-cuphead-itunes/> & <https://mashable.com/2017/11/06/fake-whatsapp-app-google-play-store-android/?europa=true>