ALL SAINTS'
CATHOLIC VOLUNTARY ACADEMY

Online Safety

Guide for Parents and Carers

www.allsaints.notts.sch.uk

ALL SAINTS'

Tips and Advice

Understanding online safety is tricky for all ages. At All Saints' we want to try and make the internet a better and safer place for children and young people. We have collated a range of resources to help parents/carers' support with this when outside of school. We hope that this will to help you to learn more about staying safe online as a family.

For further support please visit:

CEOP Safety Centre

Keeping children safe online NSPCC

Social media advice hub Internet Matters

Contents page

Advice on how to set up Protection Controls through your broadband providers.

The 4 big internet providers in the UK – BT, Sky, TalkTalk and Virgin Media have come together to produce helpful video guides, which may help you to download and set up protection controls they offer. Full details can be found at:

https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider

Family agreement

A great way to start positive family conversations around safe and responsible internet use, and to agree clear expectations and boundaries.

Use the questions below to help guide your conversations, focusing on those most relevant for your family.

Turn over the page for a template where you can record your agreements and expectations in writing.

Things to consider

Getting started

- What do we enjoy doing online?
- What apps, games and websites do we use the most?
- What devices, tech, toys or games do we have with internet access?
- Do we already have any rules about use of tech we want to include in our family agreement?

Managing time online

- How long do we spend on our devices?
- How does it feel when we use tech for too long?
- How do know when our screen use is interfering with family life?
- What can we do to help avoid overusing tech?

Sharing

- What is or isn't okay to share online?
- What should we check before posting images and videos online?
- How do we keep personal information belonging to ourselves and others safe?
- Do we need a family email address to use when signing up to new accounts?
- Do we know how to use privacy settings and strong passwords, and why these are important?
- How can we use features like livestreaming and disappearing content safely?

Online content

- What can we do if we see something online which seems unreliable or untrustworthy?
- When is it okay to download files, games or apps, or click on a link?
- Do we know what the age requirements, or ratings, on the games and apps we use mean?
- Do we need any restrictions on making in-game or in-app purchases?
- Which websites are okay for us to use?

Communicating online

- Who can we talk/chat/play games with online? Do we only know them online, or offline too?
- How can we keep ourselves safe when communicating with people who we only know online?
- How can we be a good friend when we are online?

If things go wrong

- What can we do if we feel uncomfortable or upset by anything we see or hear online?
- What should we do if someone we only know online asks us for photos, to meet up, or to share personal information?
- Do we know where the report and block buttons are online?

To finish...

- How could parental controls help our family?
- What will happen if one of us breaks the family agreement?
- When should we review our family agreement?

Once you've talked about your family's use of technology and the internet, think about what simple steps you can take going forward. We've given some examples for different ages below...

We agree to... (Under 11s)	Who is responsible for this?
I will use my tablet for ___ mins a day.	Hannah and Izzy
I will make sure the children's favourite games are bookmarked for them to get to easily.	Nan

We agree to... (Pre-teens)	Who is responsible for this?
I will tell mum and dad when I see something that worries me.	Tom, Ella and Yasmin
I will put parental controls in place but review it as the children grow up.	Mum

We agree to... (Teenagers)	Who is responsible for this?
I will make sure all my social networking sites are private.	Amar and Yusuf
I won't post photos of our children without their permission.	Dad

Family agreement

Use this template to put your agreement down in writing. Why not display it somewhere at home like on the fridge or a noticeboard?

Top tips

1. Make sure that both adults and young people are open to changing their online behaviour as a result of your agreement.
2. Consider your tone. Are you focusing on negative behaviour or promoting positive behaviour?
3. Make sure your agreement works for your whole family and everyone is happy with it.
4. Review your agreement in the future to make sure it reflects the current needs and ages of your family.

Who is this agreement for?

We agree to...	Who is responsible for this?
E.g. Be kind and respectful online.	E.g. We will all make sure we only post kind comments.

What happens if someone doesn't follow the agreement?

How long will our agreement last for and when will we review it?

Signatures

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

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

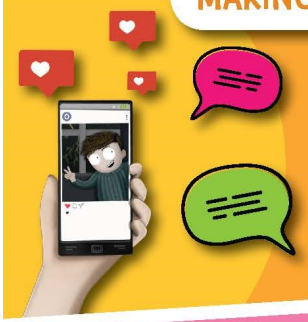
Social Media is often scrutinised as having a negative impact on children's mental health. Children and young people are now growing up in a technology dominated world, and social media plays a major role in their social lives. This balanced guide focuses on both the positive and negative impacts that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

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.

HELPFUL APPS:

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

SOURCES OF HELP:

- Childline, 0800 1111 or visit their website
- Bullying UK, 0808 8002222
- Young Minds Parents line, 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.rsph.org.uk/uploads/assets/uploaded/62be270a-a55f-4719-ad668c2ec7a74c2a.pdf, https://www.psychologytoday.com/us/blog/cutting-edge-leadership/201505/5-warning-signs-mental-health-risk

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

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?

47% of parents said they thought their children spent too much time in front of screens

What parents need to know about SCREEN ADDICTION

HEALTH & WELLBEING

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. The World Health Organisation (WHO) has officially recognised gaming addiction as a modern disease. The condition was confirmed as part of their International Classification of Diseases (ICD) which serves as an international standard for diagnosing and treating health conditions.

LACK OF SLEEP

7 out of 10 children said they had missed out 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.

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 behaviour change.

CONFIDENCE, SUPPORT & ADVICE

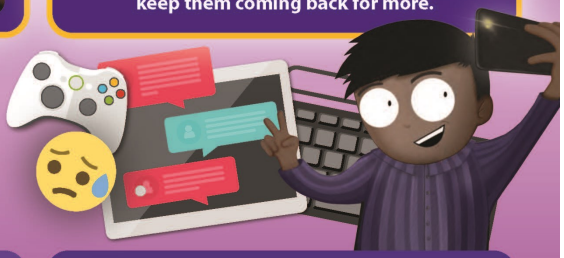
The Children's Commissioner report 'Life in Likes', explored how children aged 8-11 are using social media today. It showed that children are using their devices to speak to their online friends about their problems and seek acceptance and support, removing face to face interactions.

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 engage children and keep them coming back for more.

National Online Safety®

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 conversations and communication with their friends. 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 this, have the conversation with them to discuss why you are implementing a screen limit. There will be others 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.

ENCOURAGE ALTERNATE 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 realise they can have fun without their device. Playing football, trampolining, 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.

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. Try limiting your own screen time and follow the same rules you have set for them. If you have asked your child to not use their device at the table, make sure you don't. Try setting house rules that the whole family abide 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.

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.

REMOVE DEVICES FROM THEIR BEDROOM

Setting a rule about removing devices from bedrooms will help your child to get the sleep they need and be more focussed the next day at school. 20% of teenagers said that they wake up to check their social network accounts on their devices. Even by having a device switched off in their bedroom, they may be tempted to check for notifications.

STATISTICS

52% of children aged **3-4** go online for nearly **9hrs** a week

82% of children aged **5-7** go online for nearly **9.5hrs** a week

93% of children aged **8-11** go online for nearly **13.5hrs** a week

99% of children aged **12-15** go online for nearly **20.5hrs** a week

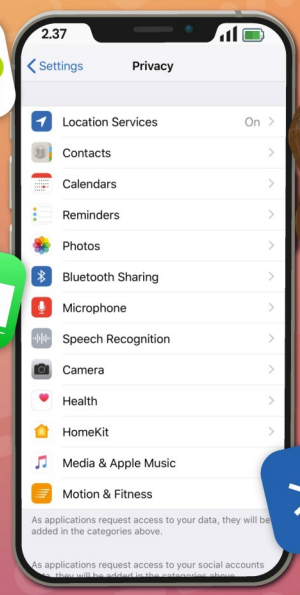
Children and Parents: Media Use and Attitudes Report 2018

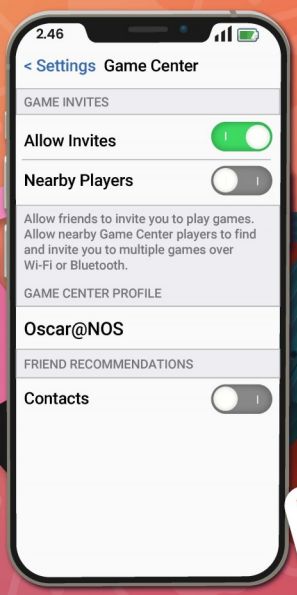
SOURCES:
https://www.independent.co.uk, Children and Parents: Media Use and Attitudes Report 2018: https://www.ofcom.org.uk, http://uk.businessinsider.com/how-app-developers-keep-us-addicted-to-our-smartphones, Journal of Youth Studies: https://www.mirror.co.uk/tech/one-five-kids-losing-sleep-9653986, University of Leeds: https://medhealth.leeds.ac.uk/news/article/1296/lack_of_sleep_damaging_for_children

How to Set up PARENTAL CONTROLS for APPS

iPhone

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





How to Restrict Built-in Apps/Features

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

How to Restrict Game Centre

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

How to Restrict iTunes & App Store Purchases

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

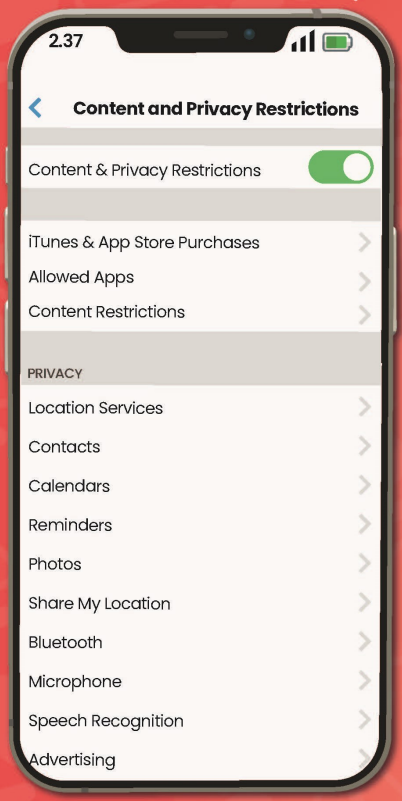
National Online Safety®
www.nationalonlinesafety.com

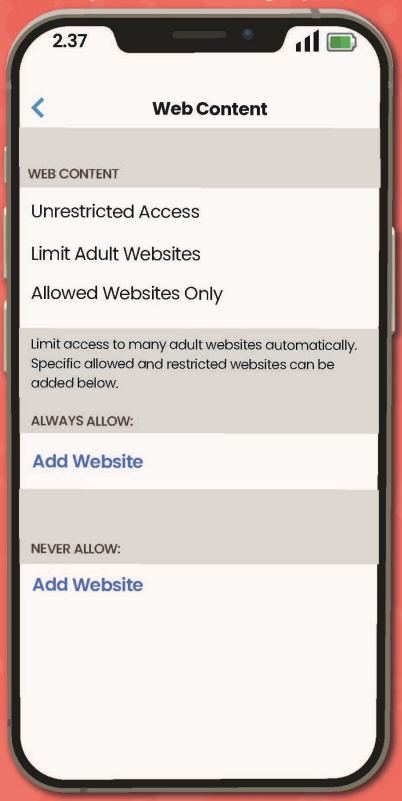
How to Set up PARENTAL CONTROLS to limit age-inappropriate CONTENT

iPhone

National Online Safety®
www.nationalonlinesafety.com

The parental controls on iPhones allow you to block or restrict certain apps, features, content, downloads, or purchases. Setting limitations on content ratings, Siri and web searches enables you to filter out age-inappropriate content and vastly reduce the likelihood of your children being exposed to unsuitable material and information.





Set up content rating restrictions

Content filters keep your child from viewing unsuitable material. They block apps, films and TV shows with specific age ratings, and music and podcasts with explicit content.

1. Open Settings
2. Tap Screen Time
3. Enable Content & Privacy Restrictions
4. Tap Content Restrictions
5. Choose the Settings for each feature you which to restrict

Set up web restrictions

Website content filters restrict age-inappropriate content on Safari. You can also blacklist certain websites or allow access only to approved sites.

1. Open Settings
2. Tap Screen TIme
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions
4. Tap Web Content
5. Choose between Unrestricted Access, Limit Adult Websites and Allowed Websites Only
7. Choose which websites you wish to allow/block

Set up Siri web search restrictions

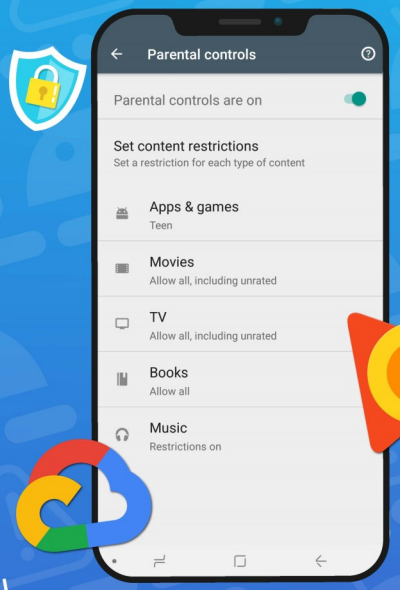
You can screen out explicit language to avoid Siri displaying inappropriate results. You could also disable Siri entirely, so your child can't use it to search the web.

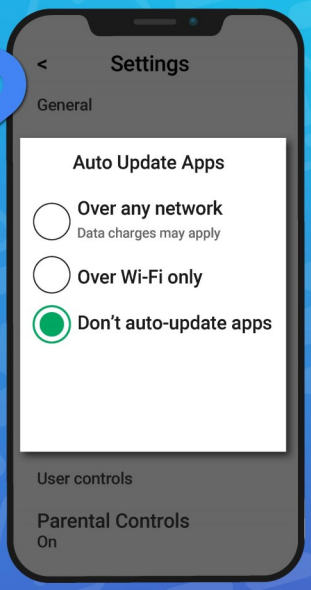
1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions
5. Scroll Down to Siri
6. Choose to block either or both Web Search Content and Explicit Language

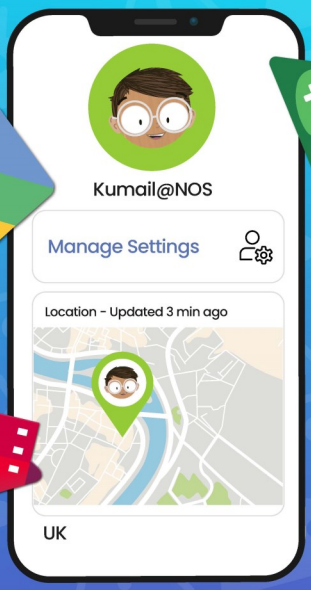
How to Set up PARENTAL CONTROLS for APPS

Android Phone

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







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

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

How to Stop Auto-updates

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

Restricting Apps Through Google Family Link

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

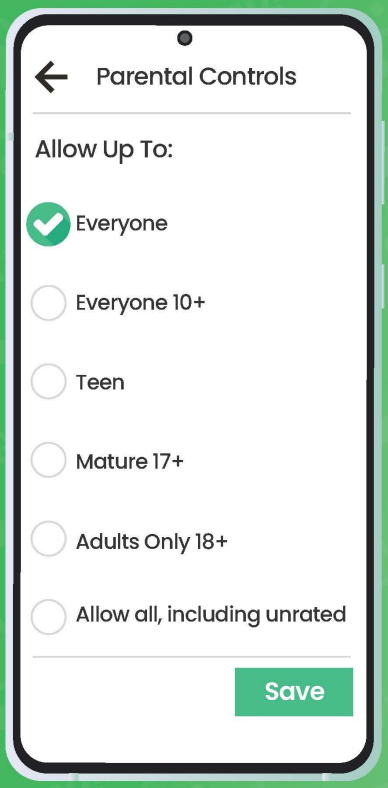
National Online Safety®
www.nationalonlinesafety.com

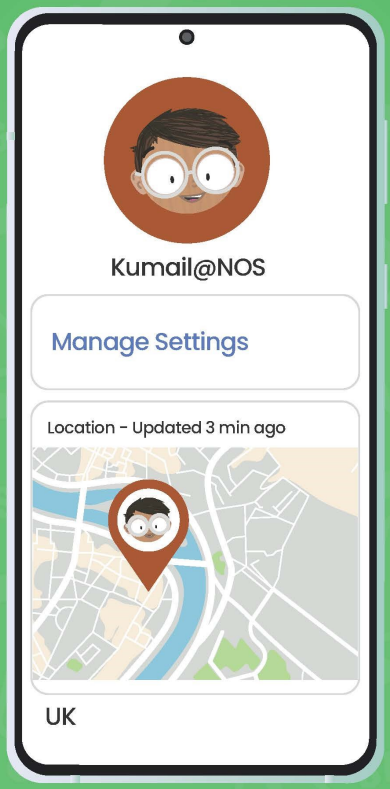
How to Set up PARENTAL CONTROLS to limit age-inappropriate CONTENT

Android Phone

National Online Safety®
www.nationalonlinesafety.com

The settings on an Android device allow you to prescribe certain rules for when your child is using it. For example, you can block specific types of content to reduce the risk of your child being exposed to age-inappropriate material (music with explicit lyrics, for instance, and games, TV shows or movies that are unsuitable for young people). There are two ways to access parental controls on an Android phone: through Google Play or via the Google Family Link app. You can also lock your changes behind a PIN, so your child (or anyone else) can't change them back.





Set up parental controls with Google Family Link

1. On your phone, install Google Family Link for Parents
2. Tap Open and review the information
3. Tap Get Started
4. Tap Next to set up your child's device
5. On your child's phone, download Google Family Link for Children & Teens and enter the Family Link setup code provided
6. On your phone, open the Family Link app
7. Tap your child's name
8. Tap Manage Settings
9. Tap Controls on Google Play
10. Tap the content you would like to restrict
11. Choose how to filter or restrict access

Set up parental controls with Google Play

1. Open the Play Store app
2. Tap Menu (represented by three horizontal lines)
3. Tap Settings
4. Tap Parental Controls
4. Enable Parental Controls
4. Create Pin
4. Tap the content you would like to restrict
4. Choose how to filter or restrict access

10 Top Tips for ...

KEEPING CHILDREN SAFE FROM CYBER CRIME

We all want to continue being informed and inspired by the ever-expanding capabilities of the internet. But we also need to be able to safeguard ourselves against the growing amount of online hazards. Knowing what is fact, understanding what dangers exist and taking appropriate steps can go a long way towards protecting yourself and your family. National Online Safety has collaborated with the Yorkshire and Humber Regional Cyber Crime Unit to compile 10 pointers to help you keep your children safe from cyber crime.

1. Spot Phishing Bait

Phishing messages are untargeted mass emails asking for sensitive information (e.g. usernames, passwords, bank details) or encouraging recipients to visit a fake website. It's safest to learn the warning signs of phishing and increase your child's awareness. Too good to be true? Spelling or punctuation errors? Odd sense of urgency? These are all red flags. Don't click on links or follow demands: if you're unsure, contact the official company directly online to enquire further.

2. Don't Over-Share

Is your child sharing too much on social media? Do they post things about their private life, upload images of your home, or discuss their friendships and relationships online? Criminals will gather this information and may try to use it for identity theft or other offences such as fraud. To combat this, ensure your child's privacy settings mean they are only sharing information with family and close friends. Use parental controls where appropriate.

3. Encourage Strong Passwords

Weak passwords make it faster and easier for someone to gain access to your online accounts or get control of your device – giving them a route to your personal information. For a strong password, national guidance recommends using three random words (e.g. bottlegaragepylons). Consider paying for your child to access a password manager. Encourage them to have a separate password for their email account. Ensure the whole family uses two-factor authentication where possible.

4. Stay Updated

People often put off installing updates to apps or software because they don't feel it's necessary, it can be time consuming, or could cause problems with programmes they rely on. But updates help protect users from recently discovered vulnerabilities to malware. You can usually set them to run automatically – encourage your child to select this option. Ensure updates are installed as soon as possible after you're notified they're available.

5. Back up Your Data

Some cyber attacks can lead to the theft or deletion of important (and possibly sensitive) data or loss of files (like photos and videos) that can't be replaced. Backing up your data to the cloud – or to another device – will help prevent data loss if you ever become the victim of a cyber attack. Where possible, set your child's devices to back up automatically. Also encourage them to back up their data prior to installing any updates.

6. Be Wary of Public WiFi

Free public WiFi is commonplace – but it's often not secure and sends unencrypted data via the network. A hacker on the same network could access personal data (like financial information) without you even realising they'd done so. To avoid this, suggest to your child that they use their 3G or 4G mobile data when they're out and about, rather than free WiFi. Consider purchasing a VPN (Virtual Private Network) where possible.

7. Take Care When Chatting

Criminals may look to manipulate others online and coerce them into using their talents or cyber skills for unethical means. Try to get your child to be open about who they are talking to online. Communication tools such as Discord are popular among gamers – but be cautious of the other people using them, and ensure you know who your child is chatting with.

8. Recognise Warning Signs

Often, budding cyber experts will relish the challenge of testing themselves or earning recognition from peers for their exploits. Even principled 'white-hat' hackers will look to test their skills online. If you think your child is interested in hacking, try to understand what their motivation is. You could encourage their participation in ethical competitions such as bug bounties.

9. Understand Their Motivations

Those being influenced online to use their skills unethically may display certain key warning signs. Sudden evidence of new-found wealth (unexplained new clothes or devices, for example), secrecy around their online behaviour or boasting of new online friendships are all causes for concern. If in doubt, refer through to your regional cyber crime team.

10. Know the Consequences

Many young people may feel that hacking is essentially a light-hearted prank, and not especially serious. So make sure your child is aware of the implications of a conviction under the Computer Misuse Act – not only the possibility of a criminal record, but also lifelong travel restrictions and damage to their future career or educational prospects.

Produced in Partnership with

The Yorkshire & Humber Regional Cyber Crime Unit (YHRCCU) works with the National Crime Agency (NCA) and other partners, in the UK and abroad, to investigate and prevent the most serious cyber crime offences.

YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT

NOS National Online Safety®

#WakeUpWednesday

What Parents & Carers Need to Know about

HOW TO COMBAT ONLINE BULLYING

Defined as "ongoing hurtful behaviour towards someone online", cyber-bullying makes its victims feel upset, uncomfortable and unsafe. In the digital world, it has numerous forms – such as hurtful comments on a person's posts or profile; deliberately leaving them out of group chats; sharing embarrassing images or videos of someone; or spreading gossip about them. Cyber-bullying can severely impact a young person's mental health ... so, in support of Anti-Bullying Week, we've provided a list of tips to help trusted adults know what to look for and how to respond to it.

1. GET CONNECTED

Playing online games together with your child or connecting with them on social media (providing they're old enough) is not only fun but also an excellent way of establishing some common ground to discuss things you've both seen or done online – as well as keeping an eye on who your child is communicating with in the digital world.

2. KEEP TALKING

Regular chats with young people about their online lives are good practice in general, but they can also be an excellent refresher to help prevent cyber-bullying situations. Topics you might want to revisit include why it's important to only connect online with people we know and trust, and why passwords should always remain secret (even from our best friends).

3. STAY VIGILANT

Observe your child while they're using technology and just after they've used it. Are they acting normally, or out of character? Possible signs of a problem may include seeming quiet or withdrawn, jumpy or anxious, angry or repeatedly checking their phone. When you feel it's the right time, you may want to check in with them to see if everything is OK.

4. MAKE YOURSELF AVAILABLE

If an online bullying incident *does* occur, it may take a while before your child is ready to open up about what happened. Just gently remind them that they can always come to you with any problems – and that they won't be in trouble. You might also suggest a trusted family member they could turn to, in case they feel too embarrassed to tell you directly.

5. BE PREPARED TO LISTEN

When conversations about online bullying *do* take place, they're likely to be difficult, emotional and upsetting for both you and your child. Actively listen to your child while they're bringing you up to speed, and try not to show any judgement or criticism – even if they haven't dealt with the situation in exactly the way you would have hoped.

6. EMPOWER YOUR CHILD

Depending on their age, your child might not want a parent 'fighting their battles for them'. In that case, talk through their options with them (blocking the perpetrator, deleting the app and so on). By allowing your child to choose the path they take, you're putting them in control but are also demonstrating that you're there to support them along the way.

7. REPORT BULLIES ONLINE

Cyber-bullying often takes place through a particular app, social media platform or online game. If this is happening to your child, encourage them to report the offender to the app or game in question – ideally with screengrabs to support their complaint. Most games and apps have reporting tools specifically to stamp out abusive behaviour and protect users.

8. ENCOURAGE EMPATHY

Protecting themselves online is the priority, of course, but young people should also feel empowered to help if they witness other people falling victim to cyberbullying. Even if they don't feel confident enough to call someone out on their abusive behaviour online, they can still confidentially report that person to the app or game where the bullying occurred.

9. SEEK EXPERT ADVICE

Victims of online bullying frequently experience feelings of isolation and anxiety, a loss of self-esteem and potentially even thoughts of self-harm or suicide. If you think that an incident of cyber-bullying has affected your child's mental wellbeing, then seek psychological support for them. There are some useful contact details in the central panel below.

10. INVOLVE THE AUTHORITIES

If the nature of any online bullying makes you suspect that your child is genuinely in imminent physical danger – or if there are any signs whatsoever of explicit images being shared as part of the bullying – then you should gather any relevant screenshots as evidence and report the incidents to your local police force.

FURTHER SUPPORT AND ADVICE

If you or your child need additional help with an online bullying issue, here are some specialist organisations that you could reach out to.

Childline: talk to a trained counsellor on 0800 1111 or online at www.childline.org.uk/get-support/

National Bullying Helpline: counsellors are available on 0845 225 5787 or by visiting www.nationalbullyinghelpline.co.uk/cyberbullying.html

The NSPCC: the children's charity has a guide to the signs of bullying at www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/ and can be reached on 0808 800 5000

Meet Our Expert

Dr Claire Sutherland is an online safety consultant, educator and researcher who has developed and implemented anti-bullying and cyber safety policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviour of young people in the UK, USA and Australia.

National Online Safety®

#WakeUpWednesday

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

What Parents & Carers Need to Know about SNAPCHAT

AGE RESTRICTION 13+

Snapchat is a photo- and video-sharing app which also allows users to chat with friends via text or audio. Users can share images and videos with specific friends, or through a 'story' (documenting the previous 24 hours) visible to their entire friend list. Snapchat usage rose during the pandemic, with many young people utilising it to connect with their peers. The app continues to develop features to engage an even larger audience and emulate current trends, rivalling platforms such as TikTok and Instagram.

CONNECTING WITH STRANGERS

Even if your child only connects on the app with people they know, they may still receive friend requests from strangers. Snapchat's links with apps such as Wink and Hoop have increased this possibility. Accepting a request means that children are then disclosing personal information through the Story, SnapMap and Spotlight features. This could allow predators to gain their trust for sinister purposes.

EXCESSIVE USE

There are many features that are attractive to users and keep them excited about the app. Snap streaks encourage users to send snaps daily, Spotlight Challenges give users to the chance to obtain money and online fame, and the Spotlight feature's scroll of videos makes it easy for children to spend hours watching content.

INAPPROPRIATE CONTENT

Some videos and posts on Snapchat are not suitable for children. The hashtags used to group content are determined by the poster, so an innocent search term could still yield age-inappropriate results. The app's Discover function lets users swipe through snippets of news stories and trending articles that often include adult content. There is currently no way to turn off this feature.

SEXTING

Sexting continues to be a risk associated with Snapchat. The app's 'disappearing messages' feature makes it easy for young people (teens in particular) to share explicit images on impulse. While these pictures *do* disappear – and the sender is notified if it has been screenshotted first – users have found alternative methods to save images, such as taking pictures with a separate device.

DAMAGE TO CONFIDENCE

Snapchat's filters and lenses are a popular way for users to enhance their 'selfie game'. Although many are designed to entertain or amuse, the 'beautify' filters on photos can set unrealistic body image expectations and create feelings of inadequacy. Comparing themselves unfavourably against other Snapchat users could threaten a child's confidence or sense of self-worth.

VISIBLE LOCATION

My Places lets users check in and search for popular spots nearby – such as restaurants, parks or shopping centres – and recommend them to their friends. The potential issue with a young person consistently checking into locations on Snapchat is that it allows other users in their friends list (even people they have only ever met online) to see where they currently are and where they regularly go.

Advice for Parents & Carers

TURN OFF QUICK ADD

The Quick Add function helps people find each other on the app. This function works based on mutual friends or whether someone's number is in your child's contacts list. Explain to your child that this feature could potentially make their profile visible to strangers. We recommend that your child turns off Quick Add, which can be done in the settings (accessed via the cog icon).

CHOOSE GOOD CONNECTIONS

Snapchat has recently announced that it is rolling out a new safety feature: users will receive notifications reminding them of the importance of maintaining connections with people they actually know well, as opposed to strangers. This 'Friend Check Up' encourages users to delete connections with users they rarely communicate with, to maintain their online safety and privacy.

TALK ABOUT SEXTING

It may feel like an awkward conversation (and one that young people can be reluctant to have) but it is important to talk openly and non-judgementally about sexting. Discuss the legal implications of sending, receiving or sharing explicit images, as well as the possible emotional impact. Emphasise that your child should never feel pressured into sexting – and that if they receive unwanted explicit images, they should tell a trusted adult straight away.

CHAT ABOUT CONTENT

Talk to your child about what is and isn't wise to share on Snapchat (e.g. don't post explicit images or videos, or display identifiable details like their school uniform). Remind them that once something is online, the creator loses control over where it might end up – and who with. Additionally, Snapchat's 'Spotlight' feature has a #challenge like TikTok's: it's vital that your child understands the potentially harmful consequences of taking part in these challenges.

KEEP ACCOUNTS PRIVATE

Profiles are private by default, but children may make them public to gain more followers. Your child can send Snaps directly to friends, but Stories are visible to everyone they have added, unless they change the settings. If they use SnapMaps, their location is visible unless 'Ghost Mode' is enabled (again via settings). It's prudent to emphasise the importance of not adding people they don't know in real life. This is particularly important with the addition of My Places, which allows other Snapchatters to see the places your child regularly visits and checks in: strangers, bullies and groomers could use this information to engage in conversation and arrange to meet in person.

BE READY TO BLOCK AND REPORT

If a stranger *does* connect with your child on Snapchat and begins to make them feel uncomfortable through bullying, pressure to send explicit images or by sending explicit images to them, your child can select the three dots on that person's profile and choose report or block. There are options to state why they are reporting that user (annoying or malicious messages, spam, or masquerading as someone else, for example).

Meet Our Expert

Dr Claire Sutherland is an online safety consultant, educator and researcher who has developed and implemented anti-bullying and cyber safety policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviour of young people in the UK, USA and Australia.

National Online Safety®

#WakeUpWednesday

Sources: Status of Mind: Social media and young people's mental health | Life in Likes – Children's Commissioners Report | https://support.snapchat.com/en-US https://netsanity.net/snapchat-parent-review/ | BT.com | Independent.co.uk; https://mashable.com/article/snapchat-status-snap-maps?europe=true, eSafety Commissioner, (2017), Young People and Sexting – Attitudes and Behaviours: Research Findings from the United Kingdom, New Zealand and Australia.

ALL ABOUT TikTok

TikTok is a video sharing social media platform used to create and share short form videos that allows users to express themselves through singing, dancing, comedy, and lip-syncing. It exploded in popularity during the COVID-19 pandemic and has only continued its rise since.

64% of young people in the UK visited TikTok in September 2021.

Over 2.5 billion installs on global devices.

1 billion global daily users by early 2022.

58% of children aged 3-15 use TikTok (alongside other social media).

THE FYP

TikTok wants users to see the content they want to see – which is where the 'For You Page' comes in. The platform uses algorithms to figure out a completely unique feed for every individual user.

ALERT
TikTok says users must be 13+ to use the app, but our research shows that it is extremely popular with younger children.

HOW IT WORKS

SHARE
Upload short videos for other users to view, comment, and like.

EDIT
Change or alter videos to include popular filters or themes.

STITCH
Use snippets of existing videos to create a new video or trend.

Use this sound

COLLAB
Add popular music or audio (including from other users) to videos.

DUET
Create a video that is posted directly alongside another user's video.

MESSAGE
Users aged 16+ can send private messages to one another.

RISKS

PUBLIC VIEWS - For users registered as 16 and over, their profile is 'public' by default and their videos can be viewed and downloaded by anyone.

INAPPROPRIATE CONTENT - Some videos include suggestive language, mature situations, and sexualised content without warning.

SCREENTIME OVERLOAD - The continuous scrolling design of the app makes it harder for users to look away from their screens, and is likely to increase screentime.

PAID ADS - Many brands and companies have taken to TikTok to try and boost product exposure with paid adverts that mix into normal content.

INFLUENCERS - Young people may be 'influenced' by popular creators on TikTok, and could spend time or money following someone or trying to become an influencer.

IN-APP PURCHASES - Users can make in-app purchases to get 'coins', which can buy virtual gifts to send to influencers on the platform.

TOP TIPS

KEEP PRIVATE. Ensure your young person's privacy settings are appropriate for their age. Remember – a private profile gives the most control!

TALK IT OUT. 'Digital life' should be as much a part of everyday conversation as every other aspect of a young person's life.

DISCUSS TOGETHER. Find out what videos and influencers they view, what they like, what they dislike – and why!

BE HONEST. Talk about how social media content is often a far from accurate depiction of real life, especially for influencers.

STAY SAFE. Some TikTok challenges could be potentially harmful to young people. Remind them that their safety is #1 always!

GIVE SPACE. Give them room to voice any concerns they might have around harmful or inappropriate content they come across.

WATCH OUT FOR... #TikTokChallenges

Hardly a day passes without a new TikTok Challenge popping up. A 'challenge' is a type of video that is widely shared and copied by others. Many of these can be fun and engaging, incorporating things like dances, songs, and filters.

There are some, however, that can be riskier and potentially harmful - which can make them even more tempting to try! These can include dangerous stunts, mean pranks, or reacting to upsetting content.

What Parents & Carers Need to Know about WHATSAPP

UK AND EUROPE 16+ 13+ REST OF THE WORLD

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

WHAT ARE THE RISKS?

SCAMS

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

DISAPPEARING MESSAGES

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

ENABLING FAKE NEWS

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

POTENTIAL CYBERBULLYING

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

CONTACT FROM STRANGERS

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

LOCATION SHARING

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

Advice for Parents & Carers

CREATE A SAFE PROFILE

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

EXPLAIN ABOUT BLOCKING

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

REPORT POTENTIAL SCAMS

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

LEAVE A GROUP

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

THINK ABOUT LOCATION

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

DELETE ACCIDENTAL MESSAGES

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

CHECK THE FACTS

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

Meet Our Expert

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

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about YOUTUBE

YouTube is a video-sharing social media platform that allows billions of people around the world to watch, share and upload their own videos with a vast range of content – including sport, entertainment, education and lots more. It's a superb space for people to consume content that they're interested in. As a result, this astronomically popular platform has had a huge social impact: influencing online culture on a global scale and creating new celebrities.

INAPPROPRIATE CONTENT

YouTube is free and can be accessed via numerous devices, even without creating a YouTube account. Some content is flagged as 'age-restricted' (requiring the user to be logged into an account with a verified age of 18), but children can still view some mildly inappropriate material. This can include profanity and violence, which some young users may find upsetting.

CONNECT WITH STRANGERS

YouTube is a social media platform which allows people to interact with other (usually unknown) users. Account holders can leave comments on any video they have access to, as well as messaging other users directly. Connecting with strangers online, of course, can potentially lead to children being exposed to adult language, to cyberbullying and even to encountering online predators.

SUGGESTED CONTENT

YouTube recommends videos related to what the user has previously watched on their account, aiming to provide content that will interest them. This is intended to be helpful but can also lead to binge-watching and the risk of screen addiction, especially if 'auto-play' is activated. Users without an account are shown popular videos from the last 24 hours, which might not always be suitable for children.

HIGH VISIBILITY

Content creators can also be put at risk – especially young ones who try to make their online presence as visible as possible. Creating and uploading content exposes children to potential harassment and toxicity from the comments section, along with the possibility of direct messaging from strangers. Videos posted publicly can be watched by anyone in the world.

TRENDS AND CHALLENGES

YouTube is teeming with trends, challenges and memes that are fun to watch and join in with. Children often find these immensely entertaining and might want to try them out. Most challenges tend to be safe, but many others may harm children through either watching or copying. The painful 'salt and ice challenge', which can cause injuries very quickly, is just one of many such examples.

SNEAKY SCAMMERS

Popular YouTube channels regularly have scammers posing as a well-known influencer in the comments section, attempting to lure users into clicking on their phishing links. Scammers impersonate YouTubers by adopting their names and profile images, and sometimes offer cash gifts or 'get rich quick' schemes. Children may not realise that these users are not who they claim to be.

Advice for Parents & Carers

APPLY RESTRICTED MODE

Restricted Mode is an optional setting that prevents YouTube from showing inappropriate content (such as drug and alcohol abuse, graphic violence and sexual situations) to underage viewers. To prevent your child from chancing across age-inappropriate content on the platform, we would recommend enabling Restricted Mode on each device that your child uses to access YouTube.

18 CENSORED

TRY GOOGLE FAMILY

Creating a Google Family account allows you to monitor what your child is watching, uploading and sharing with other users. It will also display their recently watched videos, searches and recommended videos. In general, a Google Family account gives you an oversight of how your child is using sites like YouTube and helps you ensure they are only accessing appropriate content.

CHECK PRIVACY SETTINGS

YouTube gives users the option of uploading videos as 'private' or 'unlisted' – so they could be shared exclusively with family and friends, for example. Comments on videos can also be disabled and channels that your child is subscribed to can be hidden. If your child is only uploading videos that are protected as 'private', they are far less likely to receive direct messages from strangers.

CHECK OTHER PLATFORMS

Influential content creators usually have other social media accounts which they encourage their fans to follow. Having an open discussion about this with your child makes it easier to find out how else they might be following a particular creator online. It also opens up avenues for you to check out that creator's other channels to see what type of content your child is being exposed to.

MONITOR ENGAGEMENT

YouTube is the online viewing platform of choice for billions of people, many of them children. Younger children will watch different content to older ones, of course, and react to content differently. You may want to keep an eye on how your child interacts with content on YouTube – and, if applicable, with content creators – to understand the types of videos they are interested in.

LIMIT SPENDING

Although YouTube is free, it *does* offer some in-app purchases: users can rent and buy TV shows and movies to watch, for example. If you're not comfortable with your child purchasing content online, limit their access to your bank cards and online payment methods. Many parents have discovered to their cost that a child happily devouring a paid-for series quickly leads to an unexpected bill!

Meet Our Expert

Clare Godwin (a.k.a. Lunawolf) has worked as an editor and journalist in the gaming industry since 2015, providing websites with event coverage, reviews and gaming guides. She is the owner of Lunawolf Gaming and is currently working on various gaming-related projects including game development and writing non-fiction books.

National Online Safety®
#WakeUpWednesday

What Parents & Carers Need to Know about DISCORD

AGE RATING 13+

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

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

WHAT ARE THE RISKS?

CYBERBULLYING

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

DIFFICULT TO MODERATE

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

INAPPROPRIATE CONTENT

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

ACCESSIBLE TO PREDATORS

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

CRIMINAL ACTIVITY

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

Advice for Parents & Carers

REVIEW SAFETY SETTINGS

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

EXPLAIN AGE FILTERING

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

SCREEN OUT EXPLICIT CONTENT

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

MONITOR ONLINE ACTIVITY

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

DISCUSS GOOD ONLINE BEHAVIOUR

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

HAVE CANDID CONVERSATIONS

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

Meet Our Expert

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

National Online Safety®

#WakeUpWednesday

Sources: https://www.defendyourminds.com/post/dangers-of-discord-6-steps-safeguarding-teens-on-popular-chat-app | https://support.discord.com
https://endsexualexploitation.org/articles/discord-is-a-haven-for-gamers-and-sexual-exploiters/ | https://kotaku.com/discord-deleted-thousands-of-violent-extremist-and-crim-1846623284

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

NOS Online Privacy & Security

What you need to know about...

THE DEEP WEB & THE DARK WEB

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What is it?

'The Deep & The Dark Web'

While the deep web and the dark web are not the same thing, they do overlap significantly. The Deep Web refers to pages that are not indexed, which means that most search engines (Google, Bing etc) won't return them to you after a search. The dark web is part of the World Wide Web that is only accessible by installing and using special software. It is the unregulated part of the internet; no organisation, business, or government oversees it or can apply rules. This is why the dark web is commonly associated with illegal practices.

Know the Risks

Unmonitored access

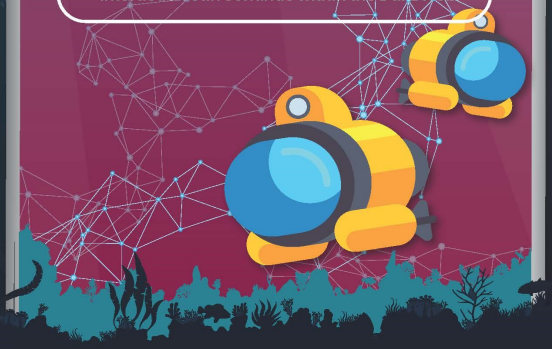
Children and young people often dive into the Dark Web using their devices, unmonitored, unregulated, and unnoticed. Whilst children may access and use the Dark Web and/or the Deep Web, a child's curiosity may result in the access and viewing of very inappropriate, unacceptable, and illegal sites, forums, and communities.

Inappropriate content

Children can access sites with indecent images, sites selling drugs and/or weapons; however, this is also the case for the Surface Web. The possibility of users infecting their devices with malware is higher when visiting the Dark Web also.

Online predators

Online child predators are more likely to interact and groom children on the Surface Web than the Dark Web. However, once contact is made, interaction can continue within the Dark Web.



Safety Tips

Question their motives

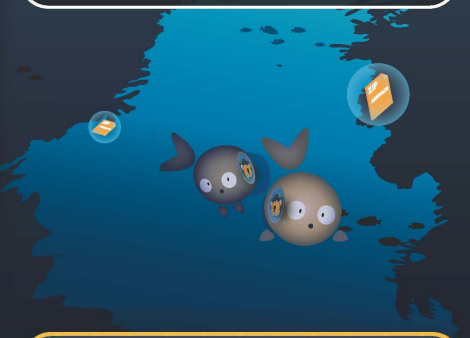
If you believe your child may be using TOR or accessing the Deep or Dark Web or asks if they can download the software, ask them why they are using them rather than using the surface web. Children should be able to access everything they need via normal web browsers.

Check devices

Check all devices for the TOR (or I2P / Freenet) software and delete any unknown browsers. Monitor your child's online purchases. If you know that your child has been using TOR to access the Dark Web, watch for any unusual mail or packages delivered to your home.

Talk about the dangers

Ask your children what they already know, and then openly speak about the Dark Web. Part of the attraction to the Dark Web may be the mystique and curiosity associated with it so it's important to educate your child about the dangers and how it can be misused by criminals.



How they Work

TOR Software

The most common software used is called TOR (The Onion Router). TOR is a web browser that keeps your identity a secret by hiding your IP address. This means that users largely cannot be tracked while browsing the dark web. Most dark web users use a search engine such as DuckDuckGo, which protects users' privacy. TOR can bypass school internet filters.

Three Web levels

The surface web is the internet we are familiar with; we use it to run businesses and connect with family, friends, and customers. Deep websites emphasise protecting users' privacy. People who need to keep their identities private use this to share sensitive information. The dark web is focused on illegal activities and services. However, unless you carry out unlawful acts, it is not illegal to use the dark web or TOR.

Our Expert

Jonathan Taylor

Jonathan Taylor is an online safety, social media and online grooming expert who previously worked as a Covert Internet Investigator with the Metropolitan Police for over 10 years. He has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, apps and platforms.

Notes

Notes

ALL SAINTS'
CATHOLIC VOLUNTARY ACADEMY

Broomhill Lane
Mansfield
Nottinghamshire
NG19 6BW
Tel: 01623 474700
Email: admin@allsaints.notts.sch.uk
Website: www.allsaints.notts.sch.uk

Through Catholic values and principles, everyone will achieve their full potential spiritually, academically, socially, morally and physically.