



Fleet Primary School

Fleet Road Hampstead London NW3 2QT

Tel: 020 7485 2028

E-mail: admin@fleet.camden.sch.uk

Headteacher: Don McGibbon



Safer Internet Day 2023

As we recognise 'Safer Internet Day 2023' today and the theme '**Want to talk about it? Making space for conversations about life online**', I wanted to share some resources and information with you:

Top Tips for Parents and Carers

These top tips have been written for you (parents and carers) to help you support your child to stay safe and happy online.

- **Make space for regular conversations about life online**

Talk openly and frequently about what you are doing online and encourage your child to do the same. Talk about the positive experiences you can have online, share what you have done when you have come across content you did not want to, and how you dealt with the situation.

- **Make space for enjoying and exploring the online world together!**

Play games, watch videos, and express an interest in your child's online life. Celebrate all the opportunities that technology has to offer, and show them what a great space the internet can be when used responsibly.

- **Make space for working as a family to agree expectations for going online**

Talk to your family about the role technology plays in your lives. Establish rules and expectations that encourage meaningful use of technology, in the same way you set boundaries in other areas of your children's lives. It's important to review these regularly and adapt them for each member of your family.

- **Make space for learning about the apps, games and websites your child is using**

There are lots of tools and guides to support you with keeping your child safe on whatever apps, games and websites they are using. Research age ratings, privacy settings, and safety features (like the block and report button) so that you are best placed to help your child should anything go wrong.

- **Make space for supporting and reassuring your child if things go wrong**

Remind your child they can talk to you about anything. If something goes wrong, listen and respond with reassurance and kindness and stay calm. Work with your child to find solutions to the problem, perhaps by using the block and report tools or seeking advice from your child's school.

Top tips for parents of under 7s

These top tips have been written for you (parents and carers) to share, and talk about, with your children. It's never too early to talk about life online!

This Safer Internet Day make space for...

- **Make space for enjoying time online together**

Play games, watch videos, and learn new skills with your child. Share what you are doing online and talk about what they like doing online. Show your child how great a space the internet can be and all of the ways you can use it as a family.

- **Make space for talking about the online world from an early age**

Show your children the amazing things they can do on the internet, before they begin to use it independently. The earlier you talk about the online world together, the easier these conversations become as they grow up.

- **Make space for using the internet to build key skills**

Why not find fun and educational games to play together, or watch videos about topics your child is interested in? The internet is a great space to practice key online safety skills like keeping your personal information safe and asking for help when you need it.

- **Make space for setting clear boundaries about tech use**

Establish expectations that encourage meaningful use of technology, in the same way you set boundaries in other areas of your children's lives. It might be no tech at dinner, blocks on certain sites, or only using devices when there is an adult in the room. Discuss these with your family, and review and adapt them as time passes and their internet usage changes.

- **Make space for familiarising yourself with safety tools**

There are loads of amazing tools and organisations to support you in keeping your child safe online. Explore the different privacy settings and [parental controls](#) available to you, and know [how to report](#) inappropriate content. These can all help make the internet a safer place for your children.

- **Make space for conversations about what to do if something goes wrong**

Reassure your child that they can always come to you if something makes them feel uncomfortable or upset while they are online. You may also like to talk to your children about putting devices down, turning them over, or pausing content if they see something they don't like.

I recognise that it can be difficult to fully monitor everything our children do when they are online – I myself have three children who all play games online and chat to their friends while they do – but it is important to keep talking with them and reminding them. When you hear them chatting ask who they are talking to. I am not going to tell you that they shouldn't play certain games but remember the advisory age ratings on games are to indicate the level of maturity a child should have before they play so that they make good, safe choices. If you are ever unsure check the PEGI rating for an app or game. Bad experiences hearing and seeing inappropriate things coming from strangers is not something our children are immune to or that only happens to others we read about in newspapers – it has and is happening with your children and you need to do what you can to keep them safe.

Being online, whether playing games, communicating with friends or finding out new things, brings a lot of joy and happiness to our children – I see that with my children – and I would urge you not to stop them doing so through worry of the issues I have raised in this letter. Instead, ensure that you know the games they are playing, who they are playing with, and remind them to come to you or another adult immediately should they see or hear anything that upsets them.

Mary Rebelo, Online Safety and Computing Consultant from the Camden Learning Centre who delivered workshops to Year 6 and Year 2 today, as well as the after school parent session, has shared this very useful 'Padlet' with lots of great links to support parents.

https://padlet.com/m_rebelo/parents-online-safety-feb-2023-q9mf5sbgoss9mdsw

You can also find more information and useful links on 'Online Safety' on the school website at:

<https://www.fleet.camden.sch.uk/learning/subject-information/online-safety>

I would also recommend highly the National Online Safety website (link below) and in particular their parent guides (I've added some for reference to the end of this letter). They post a new relevant and current guide on Twitter each week and I include them in the Wednesday school newsletter.

https://nationalonlinesafety.com/guides?utm_source=twitter&utm_medium=social&utm_campaign=nos-globaldayofparents-guides

Best wishes



Don McGibbon
Head Teacher

Tips for Encouraging Open Discussions about DIGITAL LIVES

The online world is an entirely familiar and commonplace part of life for today's children and young people, far more so than for previous generations. There are many positives to children being able to access online materials, so it's important not to demonise the internet, games and apps, and limit the benefit of their positive aspects. At the same time, we do have a responsibility to educate children about the hazards they may encounter online (just as we would about real-world dangers) so it's essential that we don't shy away from talking to them about the complex – and often sensitive – subject of what they do and what they see when they're online.

Here are some suggestions for kicking off conversations with your child about their digital life...

MAKE YOUR INTEREST CLEAR

Showing enthusiasm when you broach the subject signals to your child that you're keen to learn about the positives of their online world. Most children enjoy educating adults and will happily chat about what they use the internet for, or what games and apps they're into and how these work. Asking to see their favourite games and apps in action could help you spot any aspects that may need your attention – such as chat functions which might require a settings adjustment to limit contact with strangers. Keep listening even if your child pauses for a long time; they could be considering how to phrase something specific, or they may be gauging your reaction.

BE OPEN AND HONEST, APPROPRIATE TO THEIR AGE

At various stages, children and young people become curious about puberty and how their body changes; about relationships; about how babies are made; and about sexual health. If your child knows that they can discuss these sensitive subjects with you, they tend to be less likely to go looking online for answers – which can often provide them with misleading information and, in some cases, lead to them consuming harmful content. Don't worry if you don't immediately know the answers to their questions – just find out for yourself and go back to them once you have the facts.

REMAND YOUR CHILD THEY CAN ALWAYS TALK TO YOU

In my role I work with many children and young people who admit being reluctant to tell a trusted adult about harmful content they've viewed online, in case it leads to having their devices confiscated. Emphasise to your child that you're always there to listen and help; reassure them that if they do view harmful content, then they are not to blame – but talking about it openly will help. Children shouldn't be expected to be resilient against abuse or feel that it's their job to prevent it.

KEEP TALKING!

The most valuable advice we can give is to keep talking with your child about their digital lives. You could try using everyday situations to ask questions about their online experiences.

DISCUSS THAT NOT EVERYTHING WE SEE ONLINE IS REAL

Here, you could give examples from your own digital life of the online world versus reality – for example, those Instagram posts which show the perfect house: spotlessly clean, never messy and immaculately decorated. Explain to your child that there are many other aspects of the online world which are also deliberately presented in an unrealistic way for effect – such as someone's relationship, their body, having perfect skin and so on.

TRY TO REMAIN CALM

As much as possible, try to stay calm even if your child tells you about an online experience that makes you feel angry or fearful. Our immediate emotions frequently influence the way we talk, so it's possible that your initial reaction as a parent or carer could deter a child from speaking openly about what they've seen. Give yourself time to consider the right approach, and perhaps speak with other family members or school staff while you are considering your next steps.

CREATE A 'FAMILY AGREEMENT'

Involving your whole household in coming up with a family agreement about device use can be immensely beneficial. You could discuss when (and for how long) it's OK to use phones, tablets, consoles and so on at home; what parental controls are for and why they're important; and why it's good to talk to each other about things we've seen or experienced online (both good and bad). Explaining your reasoning will help children to understand that, as trusted adults, we want to make sure they are well informed and kept safe. Allowing children to have their say when coming up with your family agreement also makes them far more likely to stick to it in the long term.

Meet Our Expert

Rebecca Jennings of RAISE (Raising Awareness in Sex Education) has almost 20 years' experience delivering relationships and sex education and training to schools, colleges and other education providers. A published author on the subject, she also advises the Department of Education on the staff-training element of the RSHE curriculum.



National Online Safety®

#WakeUpWednesday



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.02.2023

12 Top Tips for BUILDING CYBER RESILIENCE AT HOME

As a society, we're increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off; streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops ... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It's essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS 'CYBER RESILIENCE'?

Cyber resilience focuses on three key areas: reducing the likelihood of a cyber attack gaining access to our accounts, devices or data; reducing the potential impact of a cyber incident; and making the recovery from a cyber attack easier, should we ever fall victim to one.

1. PASSWORDS: LONGER AND LESS PREDICTABLE

The longer, less common and predictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre's 'three random words' guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS

When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you've signed up for. If cyber criminals gain access your username and password for one site or service, they'll definitely try them on others.

3. USE A PASSWORD MANAGER

A good way to juggle different passwords for every site or service you use is to have a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, iPassword and Keeper are all excellent password managers.

4. BACK UP YOUR DATA

Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it's extremely important or sensitive information, you could even decide to keep more than one back-up version – by saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they do manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY

Some services let you set 'recovery questions' – such as your birthplace or a pet's name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals' task far harder.

7. SET UP SECONDARY ACCOUNTS

Some services provide the facility to add secondary accounts, phone numbers and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you're having trouble logging in or if you're trying to take back control of your account after a cyber attack.

12. STAY SCEPTICAL

Cyber criminals commonly use various methods, including emails, text messages and social media posts. Be cautious of any messages or posts that are out of the ordinary, offer something too good to be true or emphasise urgency – even if they appear to come from someone you know.

11. KEEP HOME DEVICES UPDATED

Download official software updates for your household's mobile phones, laptops, consoles and other internet-enabled devices regularly. Security improvements and fixes are a key feature of these updates – so by ensuring each device is running the latest version, you're making them more secure.

10. CHANGE DEFAULT IOT PASSWORDS

Devices from the 'Internet of Things' (IoT), such as 'smart' home appliances, are often supplied with default passwords. This makes them quicker to set up, but also less secure – criminals can identify these standard passwords more easily, so change them on your IoT devices as soon as possible.

9. CHECK FOR BREACHES

You can check if your personal information has been involved in any known data breaches by entering your email address at www.haveibeenpwned.com (yes, that spelling is correct!). It's useful if you're worried about a possible attack – or simply as motivation to review your account security.

8. KEEP HAVING FUN WITH TECH

Consider our tips in relation to the gadgets and online services your household uses. Protect yourself and your family, and don't let the bad guys win: devices are not only integral to modern life but also a lot of fun – so as long as you keep safety and security in mind, don't stop enjoying your tech.

Meet Our Expert

Garry Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.



National Online Safety®

#WakeUpWednesday

Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word | <https://haveibeenpwned.com>



www.nationalonlinesafety.com



@natonlinesafety




/NationalOnlineSafety




@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 25.01.2023



National Online Safety
#WakeUpWednesday




Online Safety Tips For Children

Do's






- 1 KEEP YOUR PERSONAL INFORMATION PRIVATE ONLINE**
Only share it with people you know like friends and family. Ask a trusted adult, like your teacher or a family member, to help you change your privacy settings so that strangers can't see it.
- 2 SPEAK POLITELY AND BE KIND TO OTHERS WHEN YOU SPEAK TO THEM ONLINE**
Treat them like you would treat them in real life and always remember your manners.
- 3 TELL A TRUSTED ADULT IF YOU ARE BEING BULLIED ONLINE**
If other another person is sending you nasty messages, a trusted adult will be able to help you collect evidence and report the person to the relevant authorities.
- 4 USE PASSWORDS TO PROTECT YOUR PERSONAL INFORMATION**
Ask a trusted adult to help you create a password that you can easily remember but which is hard for other people to guess.
- 5 ALWAYS CHECK WITH A TRUSTED ADULT FIRST BEFORE USING A DEVICE OR DOWNLOADING A NEW APP**
This is so that they can check it is safe for you to use and make sure the privacy settings are right.
- 6 TELL A TRUSTED ADULT IF YOU SEE SOMETHING ONLINE WHICH YOU DON'T LIKE**
This can include anything that upsets you, makes you feel sad or which you're unsure about.
- 7 USE THE INTERNET TO HAVE FUN AND TO HELP YOU FIND OUT INFORMATION ABOUT THINGS**
Remember to ask your trusted adult for help and always use child friendly search engines so that the information you get back is safe.




Don'ts






- 1 ACCEPT FRIEND REQUESTS FROM STRANGERS OR PEOPLE YOU DON'T KNOW**
Always tell a trusted adult if somebody you don't know tries to contact you online.
- 2 SPEND TOO MUCH TIME ON YOUR DEVICE**
Instead, go out and play with your friends, get some fresh air and try to exercise more. This will help you stay fit and healthy.
- 3 REPLY TO MESSAGES FROM ONLINE BULLIES OR PEOPLE WHO SEND YOU NASTY MESSAGES**
The most important thing to do is to tell a trusted adult and then block the person from contacting you.
- 4 COPY PEOPLE'S WORK ONLINE OR PRETEND IT IS YOURS**
This is called plagiarism and can get you into a lot of trouble.
- 5 BE MEAN OR NASTY ONLINE**
Behave online like you would in real life and don't post anything that can make you look like a bad person. Things that you post online can stay there for a very long time.
- 6 USE YOUR DEVICES CLOSE TO BEDTIME**
This will allow your brain to rest so that you can get a good night's sleep, stay focused at school and perform better in class.
- 7 SHARE PERSONAL INFORMATION ON THE INTERNET WITH STRANGERS**
Always tell a trusted adult if somebody you don't know asks you for your personal information.












12 Social Media Online Safety Tips FOR CHILDREN WITH NEW DEVICES

With Christmas only a few weeks away, many of you will be using social media to share your excitement with friends and family. Being active on social media is a great way to show others how much fun you're having, but it's important that you know how to use these apps safely and securely so that bad things don't happen. By following our safety tips below, you can make sure that your personal information stays private, your postings are positive and that your social media use overall is responsible, healthy and most of all enjoyable.

1 DON'T ACCEPT FRIEND REQUESTS FROM STRANGERS

Make sure that you set your profile to private so that people you don't know can't find you online. Always tell a trusted adult if a stranger or somebody you don't know sends you a message or a friend request.

2 NEVER SHARE YOUR PERSONAL INFORMATION WITH PEOPLE YOU DON'T KNOW

Keep your personal information personal. Sometime people online aren't always who they say they are and might ask you to share things that you don't feel comfortable sharing.

3 DON'T SHARE EMBARRASSING PHOTOS OR VIDEOS OF OTHERS ONLINE

This could really upset them and could get you into a lot of trouble. Always think twice before posting anything on social media and treat people online as you would in real-life.

4 NEVER SEND NAKED PICTURES OF YOURSELF TO OTHERS

This is illegal if you are under 18 and you could get into trouble with the Police. If you are being pressured by someone, always say no and tell a trusted adult. Even if you think it is innocent fun, the photo could be shared with other people and you won't be able to control who else sees it.

5 CREATE A POSITIVE ONLINE REPUTATION

Always be kind and polite when posting comments on social media and only upload pictures and videos of things you are proud of. This forms part of your digital footprint. Everything you do online can be tracked and monitored and could affect what people think of you in real-life if it is negative.

6 LIMIT YOUR SCREEN TIME

Social media can be addictive, and it is easy to keep checking newsfeeds or your notifications every 5 minutes which can affect your behaviour and stop you from doing other things. Remember to only use your phone at certain times of the day, turn notifications off at bedtime and go out and have as fun as much as possible. This will keep you fit and healthy and make you appreciate there's more to life than just what's on social media.

7 BLOCK ONLINE BULLIES

Sometimes people might say nasty things to you online or post offensive comments on your pictures or videos. If this happens, always tell a trusted adult who will help you block them from your profile and support you in taking further action.

8 REPORT INAPPROPRIATE CONTENT

If you see something on social media that you don't like, offends you or upsets you, you should always report it to a trusted adult. You should also report it to the social media app who will be able to remove the content if it is against their user policy and can block the person who posted it.

9 ONLY USE APPS WHICH YOU ARE OLD ENOUGH TO USE

Before downloading any new social media app, always check the age-rating. If you need help, ask your parent or carer to make sure that the app is safe for you to use and never download anything which you are too young for as it may contain content that isn't safe for you to see.

10 ALWAYS SECURE ALL YOUR SOCIAL MEDIA PROFILES WITH A PASSWORD

This will help to keep your private information safe and won't allow others to access your profiles without your permission. Make sure your passwords are memorable and personal to you but something which other people can't guess, and always share them with your parents just in case you forget them.

11 ASK PARENTS TO SET-UP 'PARENTAL CONTROLS' FOR SOCIAL MEDIA

When you download a social media app, you should always ask a trusted adult to help you set it up for the first time. This will help you control who sees what you post, who can contact you and make sure you are able to enjoy using the app safely and securely.

12 ALWAYS TALK TO YOUR TRUSTED ADULT IF SOCIAL MEDIA IS MAKING YOU UNHAPPY

Sometimes, social media can make us feel bad about ourselves or sad that we aren't the same as someone else or doing the same things as someone else. Remember, if you ever feel this way, it's really important to talk to your trusted adult(s) like your parents, carers, other adult family members or a teacher, all of whom will be able to support you and discuss your feelings with you to help make you feel better.

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, rivaling 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 screenshot 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. Additionally, it's important to be cautious about Shared Stories as this allows people who are not on your contact list access to the post.

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: Statista of Mind Social media and young people's mental health | Life in Use - Children's Commissioners Report | <https://support.snapchat.com/en-US> | <https://natsafety.wiki/snapchat-parent-review/> | <https://www.independent.co.uk> | <https://natsafety.wiki/snapchat-victim-snap-maps/> | <https://www.bbc.com/news/technology-55555555> | Young People and Sexting - Attitudes and Behaviour Research findings from the UK, New Zealand and Australia.



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Amended: 04.07.2022

What Parents & Carers Need to Know about



WHATSAPP

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

CLICK HERE

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

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



National Online Safety

#WakeUpWednesday



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 02.03.2022

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 changing across age-inappropriate content on the platform, we would recommend enabling Restricted Mode on each device that your child uses to access YouTube.

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



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 26.01.2022

What Parents & Carers Need to Know about

ROBLOX

Roblox is one of the most popular video games on the market. By 2020, the game's makers were claiming that more than half of children in the USA play it. As a 'sandbox' title, Roblox offers a huge amount of creative freedom: it lets players create their own gaming experiences with the Roblox Studio to build custom levels and games, which can then be shared with other players online. Roblox fosters creative thinking and enjoys a robust online community of fans.

WHAT ARE THE RISKS?

CONTACT WITH STRANGERS

Roblox encourages players to communicate online (including a group chat facility). This could expose children to risks such as scammers, online predators, harassment, griefers and more. The in-game chat has some filters, but isn't perfect: players can still send harmful messages to others – such as general hostility – while predators can reach out to children directly.

PUBLIC SERVERS

Roblox has private or VIP servers which allow people to play exclusively with their friends, but this costs money. Most Roblox players will instead be on public servers that anyone can join. Servers can host games which focus on all kinds of aspects, including direct player interaction. Some games and servers, therefore, will put children more at risk of contact from strangers than others.

ONLINE DATERS

These are also called 'ODers' and are quite common in Roblox. An ODer is an individual who joins a game with the intention of finding someone to date online – and eventually meet in person. Such online dating is against the Roblox community guidelines, but this usually doesn't deter ODers. Some player-built Roblox game worlds have even been designed with online dating specifically in mind.

IN-APP PURCHASES

Roblox is actually free to download and play, but bear in mind that there are some hidden costs. Players are encouraged to make purchases in the game, for example, using real money. People can also buy extra Robux (the in-game currency) to spend on cosmetic items in the game, and some private or VIP servers also have a cost.

Advice for Parents & Carers

SET PARENTAL CONTROLS

Roblox comes with several parental control options, which are explained well on the game's official website. It's essential to enter the correct date of birth for your child, as that allows Roblox to automatically apply the appropriate chat filters. The game also allows parents and carers to set monthly spending restrictions and monitor their child's account.

DISABLE PRIVATE MESSAGING

Roblox's private messaging function raises the risk of children being contacted by people they may not want to speak with – potentially leading to bullying, harassment, toxicity and scam attempts. The game allows you to disable messages from anyone who hasn't been added as a friend on your child's account.

PRIVATE SERVERS

If your child has some genuine friends to play Roblox online with, paying for a private or VIP server decreases the risk of contact from strangers. Even then, however, some players could invite other people – who might not necessarily be child friendly – into the private server. If your child is a Roblox fan, it's important to talk with them regularly about who they are playing the game with.

MONITOR SPENDING

If they don't understand they're using real money, it's easy for children to accidentally spend a sizeable amount in the game. Using parental controls to place limits on their spending will help avoid any nasty financial surprises. Ensuring that you have two-factor authentication on your payment accounts also makes it harder for your child to spend money inadvertently.

DEALING WITH STRANGERS

At some point in their development, your child will need to learn how to deal with strangers online. Show them how to block and report any users who are upsetting them or asking uncomfortable questions. Talking to them about what's OK to discuss – and what they should never tell a stranger online – will help them understand how to communicate with other people online safely.

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.

Sources: <https://www.theverge.com/2020/7/21/2333433/roblox-over-half-of-us-kids-joining-virtual-parties-fortnite>
<https://corporate.roblox.com/parents/>



www.nationalonlinesafety.com



@natonlinesafety



/NationalOnlineSafety



@nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 10.10.2022



What parents & carers need to know about ...

AMONG US

PEGI
7

Among Us is one of the most popular games to release in 2020. A space-themed 'social deduction game' where 4-10 players take on the guise of Crewmates, who must complete various tasks around their spaceship, while randomly selected Imposters must try their hardest to sabotage the others' efforts. The Imposters have to remain undetected through rounds of voting to win. Among Us is a game about deception which is heavily focused on players communicating with each other to succeed. Players need to look for the truth and lie to each other. Among Us is available for all platforms and it's free to play on mobile.

INAPPROPRIATE CHAT

While Among Us can be enjoyed locally via wi-fi, it is commonly played online. Between rounds, players come together to discuss who they think the Imposter is with a text chat, and it's here where children will come into contact with others. There is a profanity filter on the game as standard, but it can very easily be disabled and (like any unmoderated chat groups) children can be exposed to inappropriate, sexual or explicit language. Among Us has mods that allow for proximity voice chat (players can hear other people within a certain range of themselves). Voice chat is also possible using other software such as Discord.



IN-GAME PURCHASES

Among Us is currently available on both PC (via the gaming service Steam) and mobile devices. On the PC, the game costs a flat amount of £3.99 and has some in-game purchases, whereas the mobile version is free to play but contains adverts and in-game purchases. You can pay to remove the ads or purchase in-game cosmetic items. While these amounts are relatively low, there's still the possibility that young ones could accidentally spend lots of money on the game without realising it, as the process is complete in a couple of taps if a card is connected to your store account.



RISK OF HACKING

Among Us has been the target of hacking activity. Indeed, only recently the game's developer, Innerloth, tweeted advice that users play private games or with people they trust, in response to hacking issues. There is a risk of scam links being shared which take the player away from the platform and encourage them to enter private details, which could lead to criminals having access to credit card data and other personal credentials.



USE OF EXTERNAL APPS

There are many Among Us dedicated groups on Discord for voice chat with each other while they're playing. The problem with this is that it is unregulated by the game. Usually on Discord, players will only talk to other people they know in private chats, but a stranger could add a child on an external app: pretending to be interested in playing Among Us with them, when in reality they could be attempting to bully, groom or extort. Hackers will also create fake software that looks similar or identical to legitimate software to steal information. Like above, users enter their username and password which hackers then steal. For internet savvy users, this is not a problem.



MILD VIOLENCE

The art style of Among Us is cartoony but does contain some very mild violence. Imposters must kill off Crewmates one by one and can do this in a number of different ways. Some younger children might find this uncomfortable and could get scared or become upset when an Imposter is chasing them, or if they are the Imposter and are forced to kill. An age rating of PEGI 7 should help guide you in deciding if the game is appropriate or not.



Safety tips

PLAY WITH YOUR CHILDREN

Playing with your kids is one of the best ways to understand the game, and what makes it so popular. Among Us is free on mobile and is incredibly easy to pick up and play. It's also a great way to bond with your young ones - unless of course you're the Imposter or vote them out of the spaceship! You can do this by picking 'Local' on the main menu then 'Create Game'.

USE PRIVATE LOBBIES

ENTER LOBBY

Among Us uses private lobbies to let players keep track of who they're gaming with. Using a uniquely generated code that can be given to friends prior to a game starting, it gives parents peace of mind knowing who their kids are playing with. To get a game code, simply select 'Host', choose the game settings, press 'Confirm', then send the six-digit code at the bottom of the screen to friends to invite them.

DEACTIVATE CREDIT CARDS

Having your credit card automatically paired with any online accounts that can be accessed by children is asking for trouble. A solution could be setting them up with their own account with no credit card attached. They can still ask you when they want to make a purchase, but it's totally up to you as and when that transaction happens.



USE AN ALIAS

By default, your name on Among Us will be set to whatever name your device recognises you as. If this is your child's real name, you'll want to ensure they change it before hopping into a game. This is really easily done by clicking 'Online' on the main menu, then simply typing in a new name at the top of the screen.



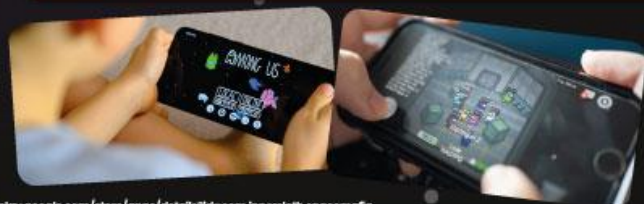
TALK ABOUT THE RISKS

It's a good idea to talk to your child about the risks associated with online gaming, especially when there are chat options and an ability to communicate with others. Try to maintain an open dialogue with your child: talk about their experiences of the game and who they're playing with. This will help you to stay on top of how they're feeling and ensure they know they can come to you if ever they feel upset or uncomfortable about anything they've experienced.



Meet our expert

Mark Foster has worked in the gaming industry for five years as a writer, editor and presenter. He is the current gaming editor of two of the biggest gaming news sites in the world, UNILAD Gaming and GAMINGBIBLE. Starting gaming from a young age with his siblings, he has a passion for understanding how games and tech work - but more importantly, how to make them safe and fun.



Sources: <https://play.google.com/store/apps/details?id=com.Innerloth.spacemafia>