

Meersbrook Bank



Community Primary
School

Year 3/4: Online Safety





- What our children are doing online
- What you can do
- Useful tools and information





- The Internet is good!
- The UK is one of the safest places to be online.
- Typically how much time do you spend looking at a screen each day?
- Be pragmatic and realistic – this is their world





What can you do?

Check if it's suitable

The age ratings that come with games, apps, films and social networks are a good guide to whether they're suitable for your child. **For example, the minimum age limit is 13 for several social networking sites**, including Facebook, Instagram, Snapchat and TikTok.

Make use of platforms and services designed with children in mind like CBBC, YouTube Kids, Sky Kids, BBC iPlayerKids. Although sites aimed at under-10s like Spotlite (Formerly Kudos) also have social networking elements. See other similar social networking sites built for kids in our ['Social networks made for kids' guide](#).





What can you do?

Check if it's suitable





What can you do?

Checklist:

Agree on boundaries

Be clear about what your child can and can't do online – where and when they can use the internet, how much time they can spend online, the sites they can visit and the type of information they can share.
Agree with your child when they can have a mobile phone or tablet.



What can you do?

Search safely

If you let your child search independently, **make sure safe search is activated on Google and other search engines**, as well as restricted mode on YouTube. You can set your default search to one designed specifically for children, such as Swiggle, and can save time by adding these to your Favourites.

The logo for Kiddle, featuring the word "Kiddle" in a colorful, rounded font where each letter is a different color: K (blue), i (orange), d (yellow), d (green), l (red), e (orange).

The logo for YouTube Kids, featuring the red YouTube play button icon followed by the text "YouTube Kids" in a bold, black, sans-serif font.





What can you do?

Stay involved

Encourage them to use their tech devices in a shared space like the lounge or kitchen so you can keep an eye on how they're using the internet and also share in their enjoyment.

REGULARLY MONITOR DEVICES

NEVER remove their device when they've seen something that wasn't their fault.

TALK TALK TALK





What can you do?

Put yourself in control

Set parental controls on your home broadband and any internet-enabled devices. Set up a user account for your child on the main device they use and make sure other accounts in the household are password-protected so that younger children can't access them by accident.

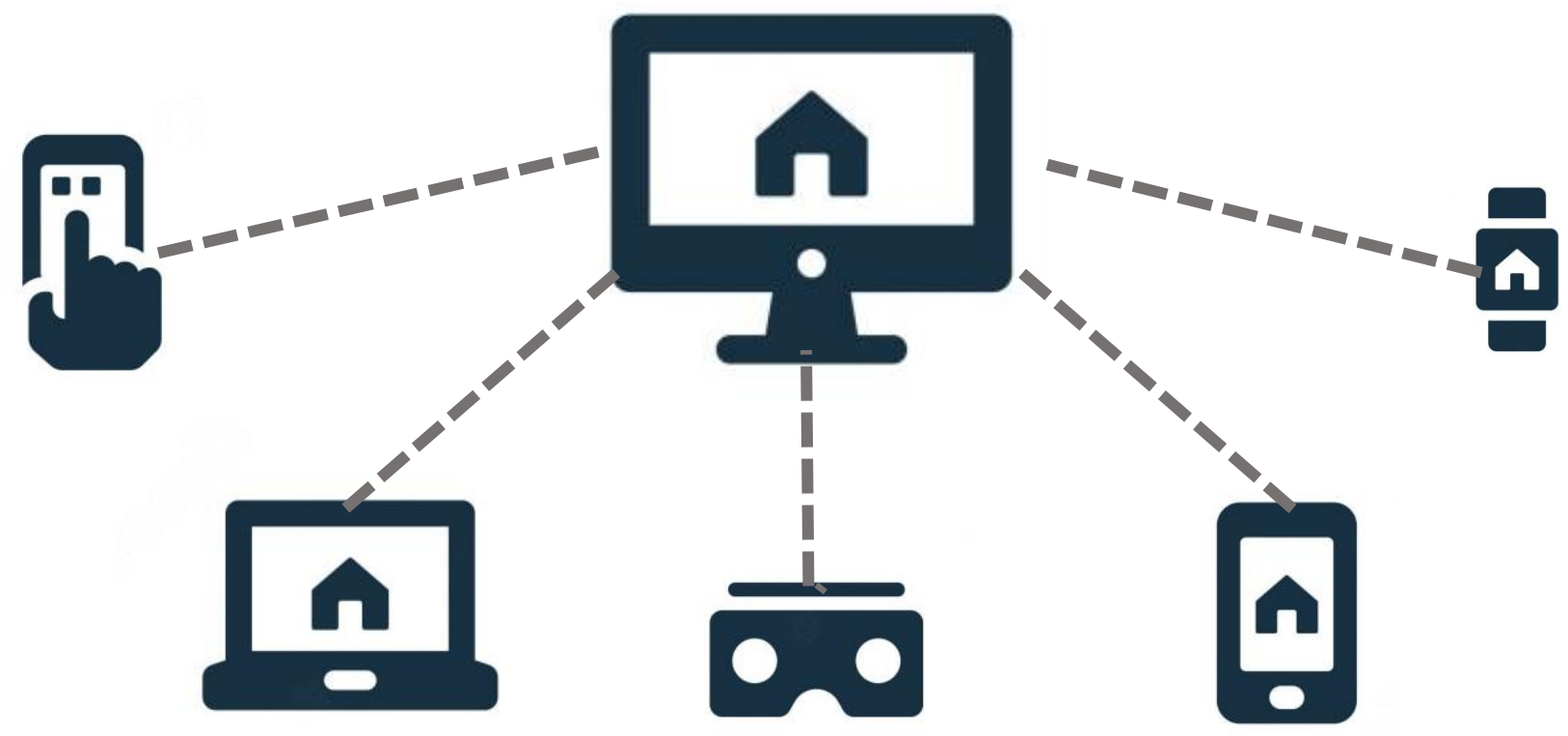
When you do give them their first device make sure that it is set up appropriately for them with the right parental controls in place. It's a good idea to **introduce tech-free meal times** and encourage them to **keep phones out of the bedroom at night** to help them build a healthy screen time balance.



Parental Controls



Parental Controls





Parental Controls



<https://www.internetmatters.org/parental-controls>



Meersbrook Bank



Community Primary
School

<https://saferinternet.org.uk>

Be in the know

You'll get knowledge, skills and tools to make the internet safer for young people at your care. Each sent once per month.

Subscribe to the UK Safer Internet Centre Newsletter



My Family's Digital Toolkit

Answer a few simple questions about your family and receive personalised online safety advice.

[GET YOUR TOOLKIT](#)

[FIND OUT MORE →](#)

<https://www.internetmatters.org/digital-family-toolkit/>





Welcome to Meersbrook Bank Community Primary School. Online Safety menu items: Dates, Letters, SEND info, Online Safety, School dinners, Uniform, Attendance, Admissions & Starting School.

https://meersbrookbank.sheffield.sch.uk/online-safety.html



Meersbrook Bank



Community Primary School



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 benefits 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...

WHY 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 showing their parents and grandparents how they use the internet, for example, for favourite games and apps. Asking to see their favourite games and apps helps you to see their interests and what they're doing. Such requests might require a settings adjustment which might require a settings adjustment. Listening to your child's interests and adjusting your time together could be a good way to keep a 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, relationships, about how bodies 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.

REMEMBER 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 a 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 shouldn't be expected to 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 perfect holiday photos which show the perfect holiday and immaculately clean, never messy and immaculately clean, never any 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 when your child tells you about an online experience that makes you feel angry or fearful. Our immediate 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 incredibly 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 see or experienced online (both good and bad). Explaining online (both good and bad) that, as well as 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

...with the information to hold an informed conversation about the safety with their children, should they feel the need to do so. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

...and therefore a key... tech and fitness... government's... in the UK. Use...

NOS National Online Safety



What can you help me report?



Threats



Impersonation



Bullying or Harassment



Self Harm or Suicide Content



Online Abuse



Violent Content



Unwanted Sexual Advances



Pornographic Content



Action Counters Terrorism: If you've seen something online that supports, directs or glorifies terrorism, report it here.

Report Terrorist Activity

We are unable to take reports of sexual images of under 18s. You can report sexual images of under 18s online directly to the Internet Watch Foundation.

Report Child Sexual Abuse Imagery



Are you being bullied?

CEOP are unable to respond to reports about bullying but if you're being bullied and would like to talk to someone in confidence right now you can speak to Childline on 0800 1111 or talk to them online - no worry is too big or too small. Please also tell an adult that you trust, like a parent/carer or teacher.

[Visit the Childline website](#) →

What kind of things do people report to CEOP?

Some of the things children and young people have reported to us include:

- ✓ Someone online has asked me to send them nude images
- ✓ I shared a nude image with someone online and they are threatening me
- ✓ I did something that I was embarrassed about on webcam and someone has turned nasty towards me
- ✓ Someone I don't know is asking me to live-stream and do things I don't want to do
- ✓ Someone online kept asking me to meet them face-to-face and I feel pressured by them
- ✓ Someone online was talking to me about sex and it made me feel uncomfortable
- ✓ Someone online is putting pressure on me to do things I don't want to do
- ✓ Someone I met in an online game keeps trying to talk to me privately

WHY?

What are the risks of WhatsApp?



Unwanted contact



Pressure to respond



Location sharing



Inappropriate content



Cyberbullying



Oversharing



Games

- Fortnite offers
- Mario Kart
- Roblox can
- Minecraft can
- Alto's Adventure



to friends.
us.
g a job or
y at school.
ngling nerves.



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.

AGE RATING

PEGI
7

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 genuine friends who they 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 others safely in the digital world.



PUBLIC SERVERS

Joining a public network (called a server) lets your child potentially interact with strangers through text chat. Some servers focus on building, while others are dedicated to role-playing – encouraging direct player interaction. Anyone can join public servers and connecting to one is relatively simple. Public server IP addresses (and therefore someone's location) are easy to find with search engines.

GRIEFING

Some people in Minecraft delight in purposefully damaging or destroying another player's creation. This is called 'griefing' and is a form of bullying: it intentionally spoils someone else's experience in the game by deleting hours of their work and forcing them to start from scratch. Many public servers treat griefing as a severe offence and frequently ban offenders.

ADDICTIVENESS

Minecraft's gameplay is relatively simple, and the outcome (when a child has built something new, for instance) can be extremely gratifying. This can make the game highly addictive. It's easy to lose track of time while playing Minecraft, causing committed young players to forget about other activities like homework or enjoying family time.

SCARY ELEMENTS

The visual design and gameplay of Minecraft is purposefully child friendly, so there's nothing too untoward in the game. However, some of the 'baddies' that can be encountered might prove a little too scary for very young players. In the game, certain enemies come out at night and are accompanied by audio – such as zombie moans and skeleton bone rattles – that may unnerve young ones.

ADDITIONAL PURCHASES

After initially buying the game, players can make optional extra purchases for cosmetic items and other bonuses. Minecraft Realms is an optional online subscription (requiring regular payments) that lets users run a multiplayer server to play with their friends. Most games consoles also need an active subscription to enable online play – so online gaming can quickly become an expensive hobby.





PERSONAL DATA

EVERY DETAIL IS KEY

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



SOCIAL MEDIA VISIBILITY

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



DANGEROUS GAMES

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



IMPOSTERS AND PHISHING ATTACKS

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



THE RISKS OF PASSWORD SHARING

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





PLAY SAFE IN ONLINE GAMES

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





Online Spending

ROBLOX



“It’s fine. My Mum’s credit card info is in. I can buy what I want whenever I want.”



Thanks for listening.