

# Internet safety at home and school

## Supporting your child at home with internet safety tips

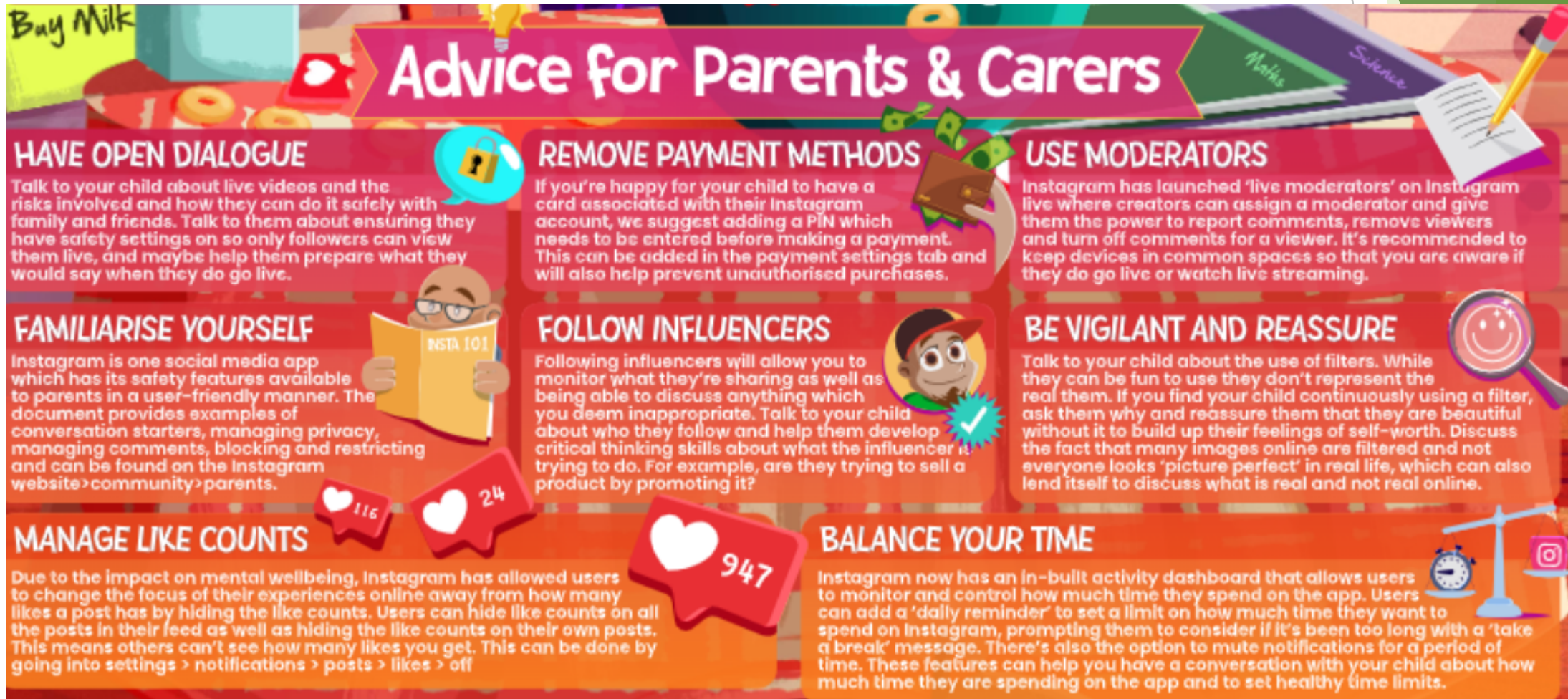


# At school

- ▶ Children are taught E-safety from Reception through to Year 6. This is revisited throughout the year to ensure children are adequately prepared.
- ▶ **Children are taught-**
- ▶ Password protection
- ▶ Protecting their identity
- ▶ Sharing information
- ▶ Videos and images online
- ▶ Games
- ▶ Online bullying
- ▶ Who to contact if they find something they do not like/makes them feel unsafe

# Instagram

## Age rating 13+





# Snapchat

## Age rating 13+

Disappearing messages make it easy for people to become victims of bullying. Screenshots can be taken, other devices can be used to photograph what has been sent

### 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).



#### 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.



#### 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.



#### 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.



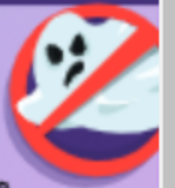
#### TALK ABOUT SEXTING

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.



#### 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).





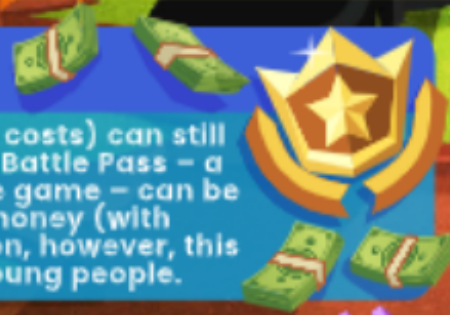
# Fortnite

Age rating 12+

## Advice for Parents & Carers

### STAY AWARE OF SPENDING

Free-to-play games (that is, ones without up-front costs) can still be big financial drains. In Fortnite, for example, the Battle Pass – a set of rewards to improve players' experience in the game – can be either earned through playing or bought with real money (with additional incentives for the latter). With supervision, however, this can be a great lesson in money management for young people.



### ENCOURAGE BREAKS

Gaming sessions can reach marathon lengths, especially when your child is on a winning streak and doesn't want to stop. Sitting in the same position for hours isn't healthy, of course, but it's an easy habit to form. Encouraging young ones to break regularly for drinks and so on will help them stay hydrated, rest their eyes and release some of the tension from competitive gameplay.



### TALK ABOUT TALKING

Communication is key in the squad-based Fortnite modes, and children will quickly realise that talking with team-mates online helps to increase their win rate. It's a good idea, therefore, to chat with your child first about speaking to strangers online, trading, scammers and other potential risks. Remind them that they can always come to you for help if they run into problems online.



### DISCUSS OTHER APPS

Games like Fortnite can lead on to third-party apps (Discord, for example) where players can join a voice, text or – in some cases – video chat about the game. Certain add-ons also let children talk with other players from their local area, which clearly presents a potential risk. When discussing Fortnite with your child, you might also want to ask them about other apps they use while playing.



# Roblox

## Age rating 7+

### 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.



# TikTok

Age rating 13+

## Advice for Parents & Carers

### TALK ABOUT ONLINE CONTENT

Assuming your child is above TikTok's age limit, talk to them about what they've viewed on the app. Ask their opinion on what's appropriate and what isn't. Explain why they shouldn't give out personal details or upload videos which reveal information like their school or home address. In the long run, teaching them to think critically about what they see on TikTok could help them to become social-media savvy.

### MAINTAIN PRIVACY SETTINGS

The default setting for all under 16s' accounts to 'private'. Keeping it that way is the safest solution: it means only users who your child approves can watch their videos. The 'Stitch' (which lets users splice clips from other people's videos into their own) and 'Duet' (where you build on another user's content by recording your own video alongside their original) features are now only available to over 16s. This might clash with your child's ambitions of social media stardom, but it will fortify their account against predators.

### LEARN ABOUT REPORTING AND BLOCKING

With the correct privacy settings applied, TikTok is a relatively safe space. However, in case something does slip through, make sure your child knows how to recognise and report inappropriate content and get them to come to you about anything upsetting that they've seen. TikTok allows users to report anyone breaching its guidelines, while you can also block individual users through their profile.

### ENABLE FAMILY PAIRING

'Family Pairing' lets parents and carers link their own TikTok account to their child's. Through your mobile, you can control your child's safety settings remotely – including limiting screen time, managing their ability to exchange messages (and with whom) and blocking a lot of age-inappropriate content. TikTok's Safety Centre also provides resources for parents and carers to support online safety among families. These resources can be found on their website.

### USE RESTRICTED MODE

In the app's 'Digital Wellbeing' section, you can filter out inappropriate content (specific content creators or hashtags, for instance) using 'Restricted Mode'. This can then be locked with a PIN. You should note, though, that the algorithm moderating content isn't totally dependable – so it's wise to stay aware of what your child is watching.

### MODERATE SCREEN TIME

As entertaining as TikTok is, you can help your child to manage their time on it in the 'Digital Wellbeing' section. Under 'Screen Time Management', you can limit the daily permitted time on the app (in increments ranging from 40 minutes to two hours). This preference can also be locked behind a PIN. That way, your child can get their regular dose of TikTok without wasting the whole day.



# Facebook

## Age rating 13+



**Advice for Parents & Carers**

**KEEP ACCOUNTS PRIVATE**

In the settings area, you can choose whether a Facebook profile is public or private. By far the safest option is to switch your child's to private, so they can only interact with people who they are friends with on the platform. Facebook's settings can also prevent your child's personal information (such as contact details, school name or date of birth) from appearing publicly.

**ENCOURAGE SAFE FRIENDING**

Facebook can help your child to stay connected with the people and the things that they care about. However, it's important for them to understand that they should only accept friend requests from people who they know. The key questions to consider are "has your child met them in person?" and "do they know and trust them enough to feel comfortable accepting them as a Facebook friend?"

**LEAD BY EXAMPLE**

Let your child watch you using Facebook – this will demonstrate how it can be used safely and appropriately, reducing the risk of them encountering harmful content themselves. Teach them the habit of thinking before sharing anything online and try to follow the same rules that you set for them – so if you agree time limits on your child's Facebook use, then you should stick to them, too.

**SAVVY SHARING**

Make sure your child realises that what they share online with friends can end up being shared again by others. It's important that they think about what they share online and who they share it with. Facebook's 'Audience Selector' gives users the option to filter who sees what they are sharing, whenever a status is updated, photos are uploaded or anything is posted.

**RESPECT BOUNDARIES**

Once you've talked about Facebook safety with your child, give them some space and trust them to make smart choices. Make it clear, however, that you're always open to discussing social media if they need to. In the early stages, you could occasionally review your child's social media activity with them to put your mind at rest – but take care not to become reliant on checking it every night.

**BLOCK AND REPORT**

On Facebook, you're able to report harmful content and block particular people or groups so they can't contact your child or view their profile. Before they start spending serious time on the platform, show your child how these features work and explain why they might need to be used. Facebook's Bullying Prevention Hub offers advice on dealing with harassment on the platform.

# Facebook messenger

## Age rating 13+

**Advice for Parents & Carers**

- USE ADDITIONAL SECURITY**  
Messenger's App Lock feature uses your child's fingerprint or face ID to ensure that nobody else can access their messages without permission. Messenger has also added a variety of optional tools to increase young people's safety on the app, including two-factor authentication, login alerts and filtered message requests.  

- REPORT INAPPROPRIATE BEHAVIOUR**  
If your child experiences anything negative on Messenger, you can help them report it. Facebook can then take action such as disabling the offender's account, limiting their ability to send messages or blocking them from contacting your child again. If your child doesn't want to display to others that they're online, they can switch off Active Status in the app's settings.  

- ADJUST PRIVACY SETTINGS**  
Make your child's Messenger stories visible only to their friends. Avoid adding your child's phone number (so they can't be found by someone using their number to search for them), and not syncing contacts lets your child choose who to add (or not) individually. Via Settings, you can control who appears in your child's chat list, who goes into the message request folder and who can't contact your child at all.  

- REVIEW THE CHAT LIST**  
Some parents regularly check their children's Messenger conversations (to see who they're talking to, rather than what they're talking about). While this is certainly safe, it can seem intrusive. If approached in a sensible, collaborative way, however, it can help parents and carers to keep an eye on exactly who their child is communicating with.  

- DISCUSS LIVE STREAMING**  
Talk with your child about safe and secure video calling. When setting up calls on Messenger Rooms, only invite people who your child knows and trusts. Show them how to lock a room if they don't want other people joining – and how to remove anyone they don't want on the call. Remind them about behaving responsibly during a live stream, even if it's with people they know.  

- ENCOURAGE SAFE SHARING**  
Ensure your child knows to send pictures and videos only to family and trusted friends, and not to publicly share images which compromise their location (showing a landmark near home or clothing with identifiable logos, like a school or local club crest). Encourage them to pause before sharing anything – if there's a chance it could harm their reputation (or someone else's), don't send it.  




# Whats app

## Age rating 16+

- Its end-to-end encryption means messages can only be viewed by the sender and recipient, not even whats app can read them!



**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.





# You tube

## A you tube kids is available

### 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!

# Minecraft

## Age rating 7+

### Advice for Parents & Carers

#### RESEARCH CONTENT CREATORS

There are a lots of Minecraft content creators who release helpful videos about the game on YouTube and Twitch. Not all of these, however, are suitable for children. Watching these content creators' channels yourself first is a safe way to find appropriate Minecraft videos to share with your children. This also helps you learn more about the game itself, and how your child plays it.



#### CHOOSE THE RIGHT MODE

Selecting 'Creative' or 'Peaceful' mode allows children to play Minecraft without having to contend with enemies. It's also a great way for you to get used to playing the game with them, since the difficulty level is lower. This allows you to work together on a long-term project, creating something special without the threat of moaning zombies or creepers damaging your build.



#### HOST A PRIVATE SERVER

The easiest way to find a safe server for your child to play on is to make one yourself. Hosting a server prevents strangers from finding it, unless they've been given the necessary joining details. A private server also lets you control who's allowed to enter and – if necessary – to ban someone who shouldn't be there. This is the closest equivalent to parental controls in Minecraft.



#### ENCOURAGE BREAKS

It's easy for the hours to fly by while your child is playing Minecraft, so reminding them to take regular breaks is essential. This is a useful way for them to learn good time management, which they'll benefit from as they get older. It will also teach them to play their favourite games in moderation – limiting addictive behaviour and allowing them to manage their day better.



#### TALK ABOUT STRANGERS

At some point in their lives, almost everyone needs to have contact with a stranger online. Talking to your child about online safety, therefore, is essential – as is having a plan in place for dealing with any hostile or difficult strangers. Ensure that your child knows never to tell a stranger about themselves online, and that they should come to you straight away if they do encounter a problem.





# Speak with your child about how they use the internet

## ► Conversation starter ideas

- Ask your children to tell you about the sites they like to visit and what they enjoy doing online.
- Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and [how to report](#) or block on the services they use.
- Encourage them to help. Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
- Think about how you use the internet as a family. What could you do to get more out of the internet together and further enjoy your lives online?



# Talking with your child

## Conversation starters

- ▶ 1. “You can always come to me if you need help.” This is the most important thing to let your child know, and a way to give them confidence to speak to you when they need support.
- ▶ 2. “What would you do if this happened...?” Give your child strategies to deal with upsetting experiences online.
- ▶ 3. “Remember that not everyone is who they say they are online.” Remind your child to always tell an adult if anyone they only know online makes them feel uncomfortable, or asks to meet up or share personal information or images.
- ▶ 4. “Keep your personal information safe, and other people’s too.” This includes full names, contact details, and real-time locations.
- ▶ 5. “Be respectful to others online.” Remind them if it’s not okay offline...

- ▶ 6. “Think before you post.” Help your child to be aware that their online actions can have consequences for themselves and others.
- ▶ 7. “Remember to ask if it’s okay.” Asking for, and receiving permission from others online is important before sharing images, adding people into group chats, etc.
- ▶ 8. “Remember not everything is true online.” Help your child to be a critical thinker to find accurate information.
- ▶ 9. “The things other people post online might not always show what their life is really like.” Reassure your child that nobody’s life is as perfect as it may seem online, and judging yourself against other’s online lives isn’t a fair comparison.
- ▶ 10. “Recognise how going online makes you feel and take a break when you need to.” Your child may need support in doing this, such as timers and reminders.

# What to do if your child has seen, or been involved in, a viral scare or suicide challenge?

- ▶ Understandably you may be distressed or angry if you hear that your child has seen, or been involved in, a viral scare/suicide challenge. It's important to stay calm, take their concerns seriously and reassure them that they have done the right thing by telling you.
- ▶ Reassure them that it is not real and that it has been put online to frighten people. [BBC Own It](#) have made a video which explains this clearly for young people.
- ▶ Remind them that when they do see something upsetting or worrying that they are in control. They can report it to the platform they are using and close down their app or browser.
- ▶ Talk to them about other sources of support – speaking to you will have helped, but further support from other sources could also help. There are [lots of organisations](#) out there can provide this.



# Parental controls

## Where can I find them?

- ▶ There are four main places you can find parental controls, and it can help to set up a combination of these:
- ▶ **Internet provider:** You can set up filters to help block access to inappropriate content on any device that connects to your home WiFi.
- ▶ **Mobile operator:** Filters are often automatically set up on mobile contracts, especially if the user is under the age of 18, but you can double-check with your provider.
- ▶ **Devices:** Many devices have parental control settings, for example, to help restrict spending in apps, reduce screentime, or disable location functions.
- ▶ **Online Services:** Sites like BBC iPlayer and YouTube have parental control settings to help restrict access to inappropriate content.

# Useful links

- ▶ <https://www.thinkuknow.co.uk/parents/Listing/?cat=&ref=4765#mMain>
- ▶ <https://www.childnet.com/help-and-advice/parental-controls/>
- ▶ <https://nationalonlinesafety.com/guides>