

# Online Safety



FORESTERS PRIMARY SCHOOL

## Online safety

Computers and the internet are now a part of everyday life in our modern society. Many children use computers and mobile devices to play games, learn and explore, as well as the significant role this can play in delivering their learning in school – never more so than during times of home learning.

Whilst the internet can be a great resource and tool for education, fun, communication, and curiosity, it is important to be aware that online activity also contains potential risks such as inappropriate or harmful content, sharing/exposure of personal information and online bullying.

Understanding and discussing with your child what they are doing online is an important role for parents and carers to play. We believe that it is not only important to teach children about online safety at school, but also to support good online practices at home. This guide is intended to help you with this. Working together, we aspire to teach our children how to be safe and responsible digital citizens, who make sensible and informed decisions about their actions online.

## 8 steps to keep your child safe online [from thinkuknow.co.uk]

### 1. Explore together:

Ask your child to show you their favourite websites and apps and what they do on them. Listen, show interest and encourage them to teach you the basics of the site or app.

### 2. Chat little and often about online safety:

If you're introducing them to new learning websites and apps while school is closed, take the opportunity to talk to them about how to stay safe on these services and in general. Ask if anything ever worries them while they're online. Make sure they know that if they ever feel worried, they can get help by talking to you or another adult they trust.

### 3. Help your child identify trusted adults who can help them if they are worried:

This includes you and other adults at home, as well as adults from wider family, school, or other support services who they are able to contact at this time. Encourage them to draw a picture or write a list of their trusted adults.

### 4. Be non-judgemental:

Explain that you would never blame them for anything that might happen online, and you will always give them calm, loving support.

### 5. Supervise their online activity:

Keep the devices your child uses in communal areas of the house such as in the living room or kitchen where an adult is able to supervise. Children of this age should not access the internet unsupervised in private spaces, such as alone in a bedroom or bathroom.

### 6. Talk about how their online actions affect others:

If your child is engaging with others online, remind them to consider how someone else might feel before they post or share something. If they are considering sharing a photo/video of somebody else, they should always ask permission first.

### 7. Use 'SafeSearch':

Most web search engines will have a 'SafeSearch' function, which will allow you to limit the content your child can access whilst online. Look out for the 'Settings' button on your web browser homepage, which is often shaped like a small cog.

## 8. Parental controls:

Use the parental controls available on your home broadband and all internet enabled devices in your home. You can find out more about how to use parental controls by visiting your broadband provider's website.

Download the SMART Rules poster here:

- [SMART-rules-poster.pdf](#)

**BE SMART ONLINE**

**S SAFE** Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

**M MEET** Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**A ACCEPTING** Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

**R RELIABLE** You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

**T TELL** Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or [www.childline.org.uk](http://www.childline.org.uk)

**BE SMART WITH A HEART** Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

[WWW.CHILDNET.COM](http://WWW.CHILDNET.COM)

Registered in charity no. 109773  
© Copyright 2012 Childnet International

## Parental controls

Controlling the settings on your child's device can be a useful tool as part of your strategy to keep them safe.

Methods for doing this can vary from device to device. However, if you visit this website, you will find pull-down menus for you to select the particular device being used, and in each case a step-by-step guide to applying parental controls is provided, with pictures/screenshots and simple instructions to guide you through the process:

- [Internet Matters: Parental Controls](#)

An information sheet about setting up new devices for children is supplied here:

- [Online safety tips for children with devices.pdf](#)

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

# Online Safety Tips FOR CHILDREN WITH NEW DEVICES

The current generation are the first children to grow up in a world where digital devices are the norm. Recent studies have found that 88% of British 12-year-olds have a smartphone. Four out of ten 6-year-olds own a tablet. And almost two-thirds (64%) of children aged 8-11 use a games console. It's now rare to find a child who doesn't regularly use internet-enabled technology. Each new device means exciting new corners of the digital world to explore – and, unfortunately, new risks to be aware of.

We've put together our top tips to help you guide your children in enjoying new digital devices safely and responsibly.

- 1. ALWAYS SET A PASSWORD**  
If your child's new device has a password protection feature, use it! It helps to keep their private information safe and will deny others access to their device without permission. Your children's passwords should be something memorable to them – but something which other people can't guess (it's also a good idea for parents to write it down in case it gets forgotten!).
- 2. SET UP PARENTAL CONTROLS**  
This really is an essential when your child gets a new device, so they're protected from the outset. Most phones, tablets and consoles allow you to customise their settings to determine which games your child can play, how they can communicate (and who with), what content they can access and so on. It will give you peace of mind that they can't unintentionally do something they shouldn't.
- 3. PAY ATTENTION TO AGE RATINGS**  
One of the first things children want to do with a new device is play games and explore apps. Before they download anything or install a new console game, check its age rating. Many popular games and apps have content that's not suitable for younger ages. The safest long-term solution is to adjust the device's settings so they can only download and use games and apps appropriate for their age.
- 4. KEEP NUMBERS AND DEVICES PRIVATE**  
Make sure your child understands that they should never share their phone number with someone they don't know or accept a friend request from them. They should also appreciate that it's a good idea to mainly keep their device out of sight, never lend it to a stranger, and never put it down somewhere that other people could steal it or take it to use without asking.
- 5. HAVE THE MONEY CONVERSATION**  
Before your children start using their new device in earnest, talk to them about in-app purchases and other ways that money might be spent through their device. Once they understand, you might want to agree on a spending limit and reassure them that they can come to you if they're uncertain, or if they have made a purchase by accident.
- 6. DISCOURAGE DEVICE DEPENDENCY**  
Of course, children who've just got a new device will naturally want to spend as much time on it as possible. But whether they're zapping bad guys, watching videos or connecting with friends, it's easy for them to get attached very quickly. Gently remind them that having family time, going outdoors and getting some exercise are fun, too. And the device will still be there when they get back.
- 7. EXPLAIN SECURE WIFI NETWORKS**  
Your home WiFi is protected by a password that only your family knows, whereas public networks (like those in coffee shops, for example) can be accessed by anyone. It's important that your child grasps this difference because, if they're using a portable device on an unsecured network, then a hacker could access their personal information without them even knowing.
- 8. LIMIT SCREEN TIME**  
Using a device for too long, especially just before bed, can interfere with a child's sleep quality and reduce their concentration and overall enthusiasm. It might be helpful to agree on certain times of day when they don't use their device. Most devices' settings let you set a screen-time limit, helping your child to stay fresh and focused so they can perform well at school.
- 9. ONLY PAIR WITH KNOWN BLUETOOTH DEVICES**  
Your child may want to connect to another device via Bluetooth, so they can listen to music wirelessly or share pictures and videos with nearby friends. But if they use Bluetooth to link with a device that they don't know, they're at risk of a stranger being able to see their personal information or having someone transmit a virus onto their device.
- 10. TURN LOCATION SETTINGS OFF**  
It's safest to disable the device's location services (if it's a portable device) so your child doesn't inadvertently make other people aware of where they are. You can usually do this via the device's privacy control settings. Turning location settings off not only means your child's whereabouts can't be tracked by others, it also significantly extends battery life.
- 11. STAY AWARE OF THE SURROUNDINGS**  
It's common to see adults not looking where they're going while engrossed in their phone. Children are even more easily distracted. In some cases, young people have been hit by cars or cyclists because they were staring at their device and lost track of where they were. Remind your child that screens and walking don't mix. If they need to use their device, they should stop in a safe place first.
- 12. BE THERE IF THEY NEED TO TALK**  
Even when you've made a device as secure as you can, there's still a possibility of your child seeing something that bothers them, or someone they don't know attempting to contact them. If this happens, listen to their concerns, empathise and reassure them. Once they've explained what happened, you can decide if you should take further action like blocking or reporting another user.

**NOS National Online Safety**  
#WakeUpWednesday

[www.nationalonlinesafety.com](http://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: 16.12.2020



## Social media resources

Most social media resources have a minimum age for users to sign up – which is almost always above the age range of primary school children (13+). However, it is important to be aware of the following:

- No checks are made if children sign up giving false age details claiming to be older, which some children have been known to do.
- Even without setting up a personal user account, many of these resources will still allow anybody to view content created by others – either by installing an app on a device, or by visiting a web page.
- Most of these resources were not originally set up with children in mind (hence the age restrictions for signing up) and so much of the content may be intended for an older audience.

Some of the most commonly used social media resources are as follows:

1. [Facebook](#) – has a strict 13+ age restriction, and personal accounts must be set up by any user. Sharing of photos, videos, online chat, and involvement in groups; messages can be received by complete strangers. Strong privacy settings (“Friends only”) are available, but not applied by default – you need to set these up.
2. [Tik Tok](#) – a video sharing tool which allows sharing and interaction with content posted. Requires 13+ age to sign up, but no account is needed to watch videos, which can be viewed by absolutely anybody.
3. [YouTube](#) – another video sharing tool, again with online interaction and creation of a public profile by users. Age requirement to set up an account is 13+ but although some videos are flagged as age restricted, most content can be viewed by anybody – no account needed. A child-friendly version “YouTube Kids” is available for children aged 0-12, with far greater filtering and monitoring of content, and incorporating parental controls on a child account.
4. [Instagram](#) – share videos and photos, including by live streaming, and receive comments – including those from strangers. 13+ to sign up, but content can be viewed without an account. There is no e-mail authentication when signing up for an account, so fake/multiple accounts are particularly rife. It is strongly advised to make account settings private and switch off location sharing when using this resource, which is possible but not set by default.
5. [Snapchat](#) – a social media tool heavily focused on the younger demographic; in the United States, it is claimed that 69% of all 13–17-year-olds use (or have used) this resource – and that 41% cite it as their most important online social network. Minimum age for registering is 13, and restrictions are tighter for non-members who can only view a video if an account holder sends it to them and are not able to comment or respond to them. It is strongly recommended for users to switch on “Ghost mode” to hide personal details such as their location.
6. [Twitter](#) – a resource aimed at (and largely used by) an older demographic, with a 13+ requirement to sign up. All posts are made public rather than shared with a specific group and comments can be posted with complete anonymity or fake profiles. Whilst it is easy to block others online it is equally simple for them to set up new accounts just as quickly. Setting strict privacy settings removes much of the functionality of this resource, which is largely used to communicate and share messages with people that you don’t know.

A more comprehensive guide to apps, games and social media sites can be found here:

- [Net Aware](#)

## Online video calls

Recommendations or restrictions relating to age limits exist with most resources for online video calls, so you are encouraged to take the time to read the terms for each provider that you use. Summary information about the most commonly used resources of this type is provided at the link below:

- [Online video calls](#)

## Further information

Information sheets are provided here to inform and to help you have conversations with your children about specific areas of using social media. Sharing images, playing games online, cyber bullying, livestreaming, and watching videos are included.

- [activity-sheet-livestreaming.pdf](#)
- [activity-sheet-sharing-images.pdf](#)
- [activity-sheet-social-media.pdf](#)
- [activity-sheet-viewing-videos-online.pdf](#)
- [activity-sheet-cyber-security.pdf](#)
- [activity-sheet-gaming.pdf](#)

## Useful websites:

- <https://www.thinkuknow.co.uk/parents>
- <https://www.childnet.com/parents-and-carers>
- <https://www.saferinternet.org.uk/>
- <https://www.bbc.com/ownit>
- <https://nationalonlinesafety.com/>
- <https://www.internetmatters.org/>
- <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

• -

• -

• -

• -

• -