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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about SETTING UP NEW DEVICES FOR CHILDREN

At Christmas, millions of lucky children will be excitedly ripping the wrapping off new phones, tablets, computers or consoles. However, in the rush to let young ones enjoy their shiny gadgets, many parents neglect to set these devices up safely – increasing the chances of children going online and stumbling across adult content, making expensive downloads or installing unsuitable apps. A little time configuring the device properly can save a lot of anguish later. Here are our top tips to ensure that a dream gift on Christmas morning doesn't turn into a nightmare by New Year.

PASSCODES FOR IPHONE/IPAD

If your child's getting their own iPhone or iPad, you can set parental controls that make it difficult for them to access inappropriate content or download expensive apps. Once the device is set up, go to the Settings app and tap Screen Time, then select Use Screen Time Passcode and enter a passcode. Keep it to yourself so your child can't switch the protection off.

SCREEN TIME SETTINGS ON IPHONE/IPAD

Once you've set a Screen Time Passcode, you can adjust various safety settings. You could, for example, only allow communication with people from the Contacts app, place restrictions on App Store purchases and apply age limits to movies, music and web content. There are many more protective options available within the Screen Time settings section.

FAMILY LINK FOR ANDROID

Parents can manage Android phones and tablets, as well as Google Chromebooks, through Google's Family Link app. This gives your child some independence (and their own Google account) but lets parents monitor which apps are being used, set limits on content and ensure that parental permission is required to install apps. Look for Family Link in the Google Play Store.

SET AN ADMIN ON PCS

On Windows PCs and laptops, it's important not to let your child share a general user account or be the main admin on the device. If you're booting up a new family PC or a child's own device, set it up using your own account details and you'll become the admin by default. Then set up children with their own separate account: Settings > Accounts > Family & Other Users > Add Other User.

SET WINDOWS LIMITS

Once your child's account has been created, a parent admin can go back into the Family & Other Users menu and apply limits to it. These include restricting screen time, the type of games and apps that can be installed, web filters and more. Microsoft also includes reporting tools which, for example, can email you with a weekly summary of your child's activity on the device.

TREAT AN XBOX LIKE A PC

The same control settings you use for a PC can be used to apply parental controls on an Xbox. Again, once your child is signed into the Xbox with their own account, you can then monitor and regulate their activity from a PC or web browser. Microsoft's dashboard allows you to manage voice communication through the console: so you can limit who can contact your child, for example.

ADD A CHILD TO FAMILY LINK

The easiest way to add a child's device to Family Link is to set it up with its own Google account. It's a good idea to create this before they use their new phone, tablet or Chromebook. Once they're logged in, open the Family Link app on your phone, press '+' in the top right and add a new family member using their Google account details. Then follow the on-screen instructions.

PLAYSTATION PARENTAL CONTROLS

With parental controls for the PS5, you'll need a PlayStation Network account (as the 'family manager') and the child will need their own account, which they should sign in with on the console. This all needs to be set up in advance, so you might want to do it before the big day. Go to PlayStation.com and search 'family account' for instructions.

INSTALL XBOX FAMILY SETTINGS

If you don't have a PC, but your child does have an Xbox, it might be easier to use the Xbox Family Settings app for iPhone or Android. Here, you can restrict console screen time (particularly handy if the console is in a bedroom), restrict communication and monitor the types of game being played. There's also a feature where you can allocate spending money for games or in-game purchases.

FAMILY SHARING ON A MAC

Families using a Mac get similar screen time options to iPhone and iPad users. Again, if you're setting up a Mac for a child, make yourself the main admin and add them as a user. This is handled through Apple's Family Sharing service, which not only allows you to put controls on child accounts but share apps and other purchases with them too. Search 'family sharing' at https://support.apple.com.

DISCUSS IT WITH YOUR CHILD

If you're planning to implement any kind of restriction or protection settings on your child's new device, we'd recommend having a discussion with your young one first about what these controls do, and what they are for. If you try to impose parental controls surreptitiously or with no advance warning, don't be surprised if your child tries to find a way around them.

STAY VIGILANT

It's important to remember that none of these methods is 100% foolproof. Nobody will ever invent flawless filters or parental controls – not least because what's unacceptable to some parents is perfectly acceptable to others. So although devices' parental controls will help to keep your child safe online, they work best side by side with good old-fashioned parental vigilance.

Meet Our Expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as the *Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *Newsnight*, Radio 5 Live and *ITV News at Ten*. He has two children and writes regularly about internet safety issues.

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: 22.12.2021

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 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'll help 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 @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: 18.12.2020

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 of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about SETTING UP APPS, GAMES AND SOFTWARE

Millions of new phones, tablets, laptops and games consoles will be nestling under Christmas trees this year. However, even if parents and carers have gone to the trouble of setting up these new devices and enabling the safety features, there are still potential hazards in the apps, games and software that children will want to install and use. Knowing what to look for and discussing those risks with your child may help avoid any nasty surprises this Christmas. Here are our top tips for ensuring that unwrapping this year's presents doesn't unleash any unexpected dangers.

TAKE NOTE OF AGE RATINGS

Back when most games were bought in shops, checking the age rating was easy: it was on the front of the box. Now that most games are downloaded, it's tougher – but not impossible. All reputable download stores show a game's age rating at the point of purchase, and you can check the suitability of a specific title your child wants to play at videostandards.org.uk/RatingBoard/games.

'FREE' ISN'T ALWAYS FREE

The games market has changed radically in recent years. Many titles are free to download, but then tempt players to pay for cosmetic items (as in Fortnite) or to unlock additional content. There can be huge peer pressure for children to pay for these items. Agree a budget for in-game purchases before the game is downloaded, and make sure children can't authorise in-game purchases by themselves.

DISABLE IN-APP PURCHASING

It's not wise to leave children with devices that can make in-app purchases without your permission. Ideally, set up computers, consoles and phones so child accounts need an adult's authorisation to buy anything. On shared devices (like iPads, which don't allow user accounts), check the settings to ensure that in-app purchasing requires the account holder's password, fingerprint or face ID.

CHECK THE SPECS

To avoid let-downs, check a game's specs before buying – especially for PC or Mac, where games often need a particular graphics chip or processor to work. Sites like systemrequirementslab.com can scan your computer to see if it will run certain games properly. On consoles, make sure you're buying the right version: some newer Xbox or PlayStation games won't play on older consoles.

MONITOR IN-GAME COMMS

Voice chat with friends is part of the fun of modern gaming – but danger lurks here too. Many titles have open chat systems, meaning that children could speak to strangers or hear adult language and verbal abuse when games get particularly competitive. Using a shared family area (as opposed to alone in bedrooms) for online gaming is a good way to keep an occasional ear on what's being said.

BE WARY OF GIFTS

Titles like Roblox, Minecraft and Fortnite have in-game currencies, which can be earned through progress in the game – but can also be bought with real money. A common scam is for a young player to be offered currency if they click a link, visit a certain site or contact another user directly. Warn your child about such offers; they should show you if they're in any doubt over an in-game gift.

APPS ARE AGE RATED, TOO

Like games, apps in the major stores have age ratings, too – so you can see in advance whether an app's appropriate for your child. Additionally, phones' parental control settings allow you to set age limits, preventing young ones from downloading unsuitable apps themselves. These ratings aren't infallible, however: we've seen TV apps featuring adult shows with an age rating of 3, for example.

CONSIDER STORAGE

Most apps and games will tell you in the online store how much space they need on a device. Check this carefully – especially with games, which can run into hundreds of megabytes and beyond. If you don't have enough free storage on a device to run the game or app, you won't get a refund from the store. You can normally check a device's available storage space through the settings menu.

WATCH OUT FOR IMITATORS

Even in the official stores, untrustworthy rogue apps can slip through the net. Common tricks are apps or games that have a slightly different name to the genuine article (Fortnight rather than Fortnite, for instance) or use logos which deliberately look very similar to the official app. To avoid downloading these imitations, read the app's description and check who the publisher is listed as.

LEGAL APPS THAT BREAK THE LAW

There are many apps that are perfectly legal but enable illegal activity – streaming apps which let people watch football matches, say, without paying for Sky or BT Sport. Prosecution for using such apps is rare, but they *can* lead to risky behaviour like viewing rogue streams on sites teeming with malicious links. Watch for children installing unusual apps with 'TV', 'stream' or 'sport' in the name.

IN-APP REGISTRATION

It's common for apps and games to ask users to register: entering personal details like email address, date of birth and other information you might not want your child to divulge. Ask them to get your permission before giving any personal info to an app – and consider using *your* details rather than the child's, so they're not targeted by marketing spam or put at risk of having their data stolen.

STAY UPDATED

Most games and apps are subject to regular updates, which not only offer new content and features but also provide critical security improvements. Children tend to ignore such updates – usually because they don't understand why they're important, or they simply want to get straight on with gaming. Check your child's devices periodically to make sure these updates are being installed.

Meet Our Expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as the *Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *Newsnight*, Radio 5 Live and *ITV News at Ten*. He has two children and has writes regularly about internet safety issues.

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: 14.12.2022