5 steps to get parents online ready

Learn

Build Trust

Question

Use Tools

Be Aware

The future is exciting.

Ready?

ISPCC Childline

Vodafone Ireland Foundation

5 STEPS TO GET PARENTS ONLINE READY

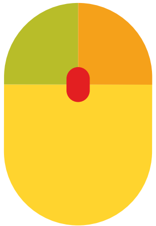
Technology and the internet present us with great potential benefits – for everything from education and schoolwork to entertainment and socialising with friends. The **Vodafone Ireland Foundation**, in partnership with **ISPCC Childline**, have developed these materials to help you to get more involved with the technology that young people enjoy so that you can understand it better and have open and informed conversations with your children.

Whether you're a parent, carer or a teacher it's all about building children's confidence and resilience so that they get the very best out of the fast-moving, ever-changing digital world.

This introductory guide will help as you start to broach the topic of internet safety with your children and will point you in the direction of useful tools, information and guidance.

Search | **Vodafone online safety**

CONTENTS



STEP 1

READY TO LEARN?

Keeping yourself informed on the latest popular apps and their functions will not only help you understand your children's online activity but also help your communication with them.

You can get familiar with the online world your children are experiencing by exploring the apps, games and social networks which they use.

This, combined with open and honest discussion with your children, will go a long way to keeping you educated on their online activities.

Social media and app trends are constantly changing. Doing a simple google search on "social media platforms being used by children" or checking what's popular in the app store will really help with this.

PEGI

TOP TIP

Did you know you can check the age ratings of social media apps or online gaming platforms to check whether they are suitable for your child. The PEGI rating provides this information across games and apps **www.pegi.info/ie**

READY TO BUILD TRUST?

Creating a trusting and open environment when it comes to online behaviours will encourage your children to share any concerns or negative experiences.

STEP 2

It can be difficult to give young people enough space to explore and do the things they want to do online while also enforcing important age-appropriate boundaries. Fear of online dangers can cause parents to become wary of the internet, which in turn can make children reluctant to share what they do online with you.

Talk to your child about the sites and social media platforms that they are using or plan to use. Take an interest in how they are using these and with whom they are engaging. An understanding of the value they place on these online interactions will help foster an honest and open conversation about online safety.

Establishing a set of household rules verbally or even in writing around internet and tech usage can contribute to this trusting relationship. It will also help you set limits around when, where and how long children can use the internet or their devices. While children may protest, they often feel safer when rules and boundaries are in place.

These boundaries will also help to maintain your child's other interests and ensure that their sleep is not interrupted by device notifications or staying up late browsing the web.

A trusting relationship will be strengthened if you lead by example. If your children notice that you are not dependent on your phone and take time to actively engage in face-to-face conversation and real-world activities, they will do the same. Being fully present when you're with your children can help to encourage them to do the same with you.

TOP TIP

Together with your child, create some written rules around online behaviours for your family to follow which could be placed in a communal area as a reminder of what you have agreed

STEP 3

Help your child to develop crucial online perception skills by teaching them to think critically and question.

What goes online can remain online. Help your children understand that words and images posted or shared online can remain there forever. Talk to them about the potential consequences of sharing photos or posts online – get them questioning whether they want the things they post to contribute to their digital footprint. A good perspective on this is to tell your children not to post or share anything online that they would not be happy with you (or their granny) seeing.

Help educate your child on 'fake news' and 'phishing' scams (fraudulent attempts to obtain sensitive information. e.g. usernames, passwords, credit card details). Encourage them not to take everything they see at face value and to start interrogating whether information is truthful and accurate. Remind them that where newspaper and TV broadcasting is developed by professional journalists, anyone can upload content to the internet.

Everyone should be conscious of the potential dangers of sharing personal information online. An important step you can take is to ensure your child understands what constitutes personal information and questions how other content can give away personal details (e.g. photos with identifiable locations or school uniforms etc.)

It's easy to have an anonymous bravado in your online personality – but make sure that when your child is chatting or posting online they are questioning whether they would feel comfortable saying the same thing to the person's face.

READY TO GET THEM QUESTIONING?

TOP TIP

Test and improve your child's (and your own) online critical thinking skills by taking some 'fake news' and phishing tests here (hyperlink to http://www.vodafone.com/content/parenting-quiz/index.html)?

READY TO USE SAFETY TOOLS?

STEP 4

Children's use of the internet presents great potential benefits – for everything from education and schoolwork to entertainment and socialising with friends. However, access to certain applications, websites and games should be age-appropriate to best protect your children from potential dangers.

There are safety features installed on most computers, tablets and phones and it is a good idea to switch these on before giving a child a device for the first time.

The settings used on social media platforms and websites can be different in each case.It's a good idea to educate yourself and your child on the following, for each one being used.

How to adjust the security and privacy settings

How to block or unfriend someone

What and where the reporting functions are

How to delete your profile or account

Some apps and social media sites have built-in location settings which can be turned on or off. If these are turned on, without the right privacy settings, it may be possible for stangers to find a child's identity and location through a social media platform. Talk to your child about their privacy settings and familiarise yourself with the different platforms they are on and how to set privacy settings.

TOP TIP

Did you know you can check settings on any apps your children have access to on their own or shared devices and ensure location services are turned off so that they are not at risk of being located or identified?

READY TO NOTICE?

STEP 5

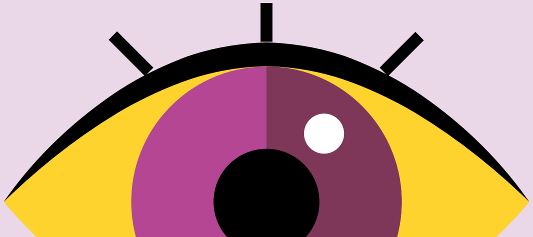
Finally, whilst it is important to remember that the positives of the internet outweigh the negatives, it is crucial to understand the potential dangers which exist online (e.g. cyberbullying, online grooming, online scams/ phishing, and accessing inappropriate content). Being on the lookout for changes in behaviour can help you detect if your child is having negative experiences online. Warnings signs vary widely, and can include:

Becoming withdrawn or moody, and refusing to talk about what they do online

Spending more time online, or refusing to go online at all

Cutting ties with friends, and showing a reluctance to go to school or extracurricular activities

Fatigue – if your child has access to their device at night this could be a reason



TOP TIP

Talking to your child is always the best first step, but if you have an ongoing concern about your child's online activity, a quick check of your family devices' browser history will give you a comprehensive list of the sites your child has been visiting.

Googling your child's name will also give an indication of what social media platforms they are active on and whether they have activated the security settings available.

TOOLS, SETTINGS AND USEFUL RESOURCES

And now for the more practical bits...

There are lots of ways to safeguard children online - the following guide will provide you with a range of information and options to help keep your children safer online. With lots of tools and options available, it's important to understand what tools and settings can do – and what they can't.

The best tool that you have as a parent is a strong relationship with your child. It is important that they understand that if something goes wrong, or they see or experience something that makes them uncomfortable, that they can come to you about it.

The following information can help, but parental vigilance in knowing what children are doing online, as you would in the real world, is key to protecting your children.

Parental controls allow you to manage your family's use of online services and devices. Mobile phone operators offer similar parental controls for handheld devices as internet service providers do for software on laptops, PCs and Macs.

Filters include services like SafeSearch on search engines. They do just what they say on the tin – restrict access to specific content. Filters are helpful if you have young children, but can restrict useful content like sex education and other health-related information. They only work on classified content and a lot of sites, including reputable ones, carry content that isn't classified, so it is possible that inappropriate content can slip through.

Settings are built into services such as WhatsApp. They help you control what other people see about you and your children.

Finally, one of the most useful tools you can use as a parent is strong, private and unique passwords for each device in your home, apps and services which your children use.

******

TOP TIP

Teach your child that passwords are like toothbrushes: not for sharing, even with their friends!

SETTING AND CHANGING PARENTAL CONTROLS ON SMARTPHONES AND TABLETS

Parental controls on tablets and smartphones can restrict specific sites and 'adult content'. Mobile phone companies can filter content rated 18+ at network level. Contact your mobile phone company to check whether this filter is on or off.

The main mobile providers (e.g. Vodafone, Three and Eir) automatically block 18+ rated content through the Active Choice network- level filtering system. But this only works if the device is connected via the mobile network, not Wi-Fi.

Your mobile's operating system may also include safety features and you can set restrictions on the App Store and Google Play.

iOS – (e.g. iPhone and iPad)

You can enable restrictions on an iPhone or iPad for access to features such as FaceTime, in-app purchases, app, and web browsing using Safari.

Firstly, to enable restrictions, open Settings and choose **General > Restrictions** to display the Restrictions window. Now tap the Enable Restrictions button at the top of the window. You'll be prompted to enter a four-digit Restrictions Passcode. Once you've set a passcode, Restrictions are turned on. You can change any of the settings in the Restrictions window to enable or disable certain features.

You can also set a specific list of websites which your child can have access to. To set up a list of allowed websites, make sure Restrictions is turned on, and open Settings. Choose General > Restrictions > Websites as you did for blocking websites and tap Specific Websites Only. You'll see a list of Apple-approved websites appear. Your child can now browse only these websites in Safari; all other websites on the internet are blocked. If you don't agree with Apple's choices and want to alter this list, you can tap Add a Website... at the bottom of the list to allow another site. You can also remove a site from the list by swiping left on the site and tapping Delete.

As with Limit Adult Content, note that this feature only works in Safari. If your child uses another browser, they'll be able to visit any website.

Another effective way to keep younger children safe on an iPad is to use Guided Access. This feature lets you lock the iPad to the currently-displayed app.

Android Phones & Tablets – (e.g. Vodafone, LG, Samsung, Sony, HTC, Huawei, Motorola, Amazon)

The Restricted User feature lets you choose which apps and content your child can access, such as the camera and Chrome web browser. Go to the setting app, select Users under the devices section and create a restricted profile. A Restricted Profile allows you to choose which apps you allow this new user to have access to, restrict content and there's no access to the Play Store so kids can't download any new apps themselves. There's also an option that allows you to decide whether to allow Location Services for that user.

Windows Phone – (e.g. Microsoft Lumia)

The My Family option helps you to manage the apps and games that your child is able to download to their phone. You can also set up Kid's Corner on your own Windows Phone so that if your child borrows your phone, they can only access age-appropriate content and not acess the rest of your stuff that you want to keep private.

SAFETY AND PRIVACY CONTROLS ON SOCIAL NETWORKS AND APPS

Facebook

Minimum age: 13

What can you set? Decide who sees your posts and Timeline, unfriend people and block people.

For more information and instructions see the 'Tools for parents and educators' page on Facebook.com

Snapchat

Minimum age: 13

What can you set? Choose who can send you Snaps, decide who can view your Stories and block people.

Instagram

Minimum age: 13

What can you set? Control your visibility (set photos and videos to private) and block people.

Twitter

Minimum age: 13

What can you set? Protect your tweets so that only approved followers can see them, hide certain users' tweets from your timeline, block people from contacting you and make use of the quality filter.

Kik

Minimum age: 13 with parental permission; 18 without

What can you set? Manage who can talk to you and block people.

ooVoo

Minimum age: 13

What can you set? Prevent certain people from contacting you, block incoming calls, prevent people from seeing your photos and set video-call privacy options.

Whisper

Minimum age: 13

What can you set? Block people and hide your location.

ASKfm

Minimum age: 13

What can you set? You can allow or block anonymous questions, block specific users, delete answers from your profile and control other users' questions appearing on your profile. Ask.fm is an anonymous question and answer platform website used regularly by lots of young people in Ireland and around the world. It allows anyone to post anonymous comments and questions to a person's profile.

WhatsApp

Minimum age: 13 with parental permission; 18 without

What can you set? Control who sees your information, what you see, who you interact with and what you share

Live streaming services

Live streaming platforms let users chat to each other or broadcast videos of themselves in real time. This can create privacy and safety issues for users of all ages, so check the settings and controls on each individual app. Here are two of the most popular streaming platforms:

Skype

Minimum age: 13 with parental permission; 18 without

What can you set? You can hide your age, date of birth and gender; only allow people in your contact list to get in touch; and block people.

Periscope

What can you set? You can hide your location; set Private Broadcast, so only people you invite can watch your broadcasts; restrict chat to only the people you follow; and choose not to share your broadcast on Twitter.

SETTING RESTRICTIONS ON APP STORES

Apple Store

To prevent your child downloading apps that are age-inappropriate, you can set up parental controls on app stores.

For Apple simply go to their support page here https://support.apple.com/en-gb/HT201304

Google Play Store

How do Google Play parental controls work? Parental controls work on Android devices where your child is signed in to their Google Account. A parent in the family group needs to use their Google Account password to set up or change their child's parental control settings.

To set up parental controls. First open the Family Link app. Select your child. On the "Settings" card, tap **Manage Settings > Controls on Google Play**. Tap the type of content you want to filter. Choose how to filter or restrict access.

Note: You can also manage this setting by clicking on your child's name at families.google.com.

Note: Parental controls don't prevent seeing restricted content as a search result or through a direct link.

GAMES CONSOLES

Games consoles have built-in parental controls, which are usually accessible through the console's home screen. These allow you to restrict users to viewing only age-appropriate games, based on the official PEGI ratings. To find out more about PEGI ratings, go to **PEGI.info/ie** You can also disable in-app purchases for some games.

You can find detailed instructions about setting up controls for the following consoles on the website of the Video Standards Council: Xbox One, Xbox 360, PS4, PS3, PS Vita, PSP, Nintendo 3DS and Nintendo WiiU. Visit gamesrating authority.org/GR A and click on 'Controls' in the top navigation bar.

PARENTAL CONTROLS ON YOUR COMPUTER'S OPERATING SYSTEM

MacOS and **Windows** both include parental controls that allow you to set time limits for your child's use and restrict access to certain types of content. In both operating systems, parents can set up user accounts for each member of the family with their own unique passwords and then tailor the controls and restrictions to the age and maturity of their child.

Windows

Windows 10 offers access controls, time limits and activity reports, including reports on the websites, apps and games your child uses. You can set up individual user accounts with different age-appropriate controls. Earlier versions also offer controls but the set-up process differs.

MacOS

Parental controls on your Mac let you add a 'managed user' so you can limit your child's access to age-appropriate websites and apps, determine who they are allowed to contact via Mail, Messages and Game Center, set time limits and block use of the computer's built-in camera.

THIRD-PARTY PARENTAL CONTROLS

You may decide to use a dedicated parental control solution to do things like set time limits and block inappropriate contect. If you already have a security suite on your computer or device, check whether it includes parental controls. You may not need a third-party one. Some are free, but most will cost you an annual subscription.

Vodafone Secure Net

McAfee Family Protection

Norton Family

Net Nanny

Qustodio

SAFETY CONTROLS ON SEARCH ENGINES

You can change the settings on the browser you use to access the Internet. But if you use more than one browser, you'll need to change the settings on each one.

Chrome: With Supervised User accounts on Google Chrome, you can allow or block certain sites,
see which websites have been visited and prevent apps being installed.

Internet Explorer: Microsoft's Content Advisor enables you to prevent your child seeing websites containing nudity, violence and other inappropriate content

Firefox: The parental controls in Firefox let you filter web content that may be inappropriate or offensive for children.

Setting **SafeSearch** on search engines means that the majority of sexually explicit videos and images will be filtered from search results, along with results that may link to explicit content. It isn't 100% reliable but is useful if you have a young child.

Restricted Mode on YouTube performs a similar function to SafeSearch – and both can be locked if you have a Google+ account. But these are device-level settings – meaning you have to set them on each tablet, phone or computer your child uses.

Google's SafeSearch setting enables you to filter out most adult content. If an inappropriate search result gets through, you can report it to them. You can also find information about safety features on YouTube, Google Play, Chrome and other services in the **Google Safety Centre**.

Other search engines, such as Yahoo and Bing, offer their own safe search options. You will usually find them under 'settings'.

SAFE MODE ON VIDEO WEBSITES

Movie and TV channels online offer a huge range of content for all the family. Some use a combination of password and PIN to set restrictions on viewing, based on age ratings. Some let you create separate profiles for child users so they can only view child-friendly content. Obviously, these restrictions only work if you keep the passwords and PINs secret

YouTube: YouTube's Restricted Mode helps to screen inappropriate content that you wouldn't want your child to see.

amazon and amazon Prime: Amazon's PIN feature lets you set purchase and viewing restrictions on your registered devices. Turn on Restrictions to limit access to specific features – such as app purchases and multiplayer games and content – on your Apple TV.

RTÉ player: Parental controls can be enabled to help prevent children from accidentally watching programmes intended for an adult audience. You must log in with your RTÉ ID to change the settings at https://login.rte.ie/rtesso/login/

sky: Using PIN-protected parental controls, you can restrict the programmes and channels your child can watch on Sky TV. In addition, the Sky Kids app contains thousands of children's shows and lets you filter them by age

NETFLIX: There are four maturity levels in Netflix parental controls (Little Kids, Older Kids, Teens and Adults) to help you control what your child watches.

YOU now: Minimum age: 13 with parental permission; 18 without What can you set? Use a nickname, hide your location and block people

We have listed select features of all services. There may be other safety or privacy settings available. If your child sees anything inappropriate or sexual on a live streaming app, they/you should report it to the site's administrators. If they are the subject of inappropriate sexual contact or approached by another person, they should tell a trusted adult and report it immediately to GNPSB (Garda National Protective Services Bureau).

USEFUL WEBSITES

The following websites and organisations provide additional and up-to-date information and resources for parents and children to stay up to date on the best ways to enjoy the online world safely.

www.childline.ie and **www.ISPCC.ie**
Support sections tailored to children and to adults respectively

www.CybersafeIreland.org
Balanced and professional guidance to schools, children and parents in the safe and responsible use of all communications technologies

www.commonsensemedia.org
Database containing thousands of apps, movies, games etc. including suggested age ratings, mini-reviews, and an indication of the app's quality,

www.Webwise.ie
Internet Safety site of The National Centre for Technology in Education.

ww.ESafety.ie
Internet and technology educational materials for parents, teachers & students.

www.h2bsafetycentre.com
Videos, prompt cards and other resources and practical advice on how to report, block and configure your settings across the most popular apps and games

www.watchyourspace.ie
Advice on how to stay safe on social networking sites.

www.gamesratingauthority.org
Detailed instructions about setting up controls for the following consoles on the website of the Video Standards Council: Xbox One, Xbox 360, PS4, PS3, PS Vita, PSP, Nintendo 3DS and Nintendo WiiU. click on 'Controls' in the top navigation bar.

www.PEGI.ie
Age ratings information and guidance to consumers (particularly parents) to help them decide whether or not to buy a particular product – game, films.

www.tacklebullying.ie
Advice from the Anti-Bullying Centre in Dublin City University

The **ISPCC** is Ireland's national child protection charity. In 2016, it commenced a major five-year partnership with The **Vodafone Ireland Foundation** with the joint mission to keep children safe by keeping them connected. A key aspect of this work is to shape national law, policy and practice in the field of child protection online.

Together we continue to develop internet safety guidance while working to drive for a national strategy on children's cyber safety including education measures, enhanced regulation, law reform and an office of digital safety commissioner.

ISPCC
Childline

Vodafone
Ireland
Foundation

Vodafone
Ireland
Foundation