Protecting children of the digital age

Everything you need to know about parental controls

WardWiz

Acknowledgements

Thank you for purchasing this guide. This book has been a long time in the making and is something that almost every parent we have spoken to is actively looking for. But this guide is just the start. We hope to be in a position to publish regular updates to our community. As new products, apps, and platforms are developed, our goal is to provide up-to-date advice on the benefits, dangers, and - of course - the safety features to ensure your children can enjoy the internet safely.

I'd like to personally thank Jason O'Mahony for his time, dedication, and effort, as well as each and every one of you who have given so much support and encouragement over the last five years. We are fully committed to ensuring the protection of children online and the education of parents regarding the many possible dangers in the online world. Unfortunately, for now, we cannot change the web, so it's important we change our own online behaviours to ensure we minimise the potential risk of harm to both adults and children alike.

A message to parents

The internet may be one of humanity's greatest creations. Think of the endless opportunities, the people across the world you can connect with, the many ways you can enrich your life. From your desk at work you can visit every corner of the world and see all the beauty it holds. You can learn skills you would have never dreamed of. In every corner, you can find a new friend willing to show you a glimpse into their world. The internet can be a tool for so much good.

Unfortunately, there are two sides to the coin. For all the good, there's an equal amount of bad.

In a world of trolls, catfish, fake accounts, and Facetune, the internet is a dangerous place for everyone not on their guard. And children are the most at threat. If you take your eye off what they're doing, they can unwittingly walk into an unsavoury individual - someone with nothing but bad intentions. This isn't to scare you into banning the internet from your house, nor to suggest everyone is like this. But it only takes one person to make a lifelong impact on your child's life.

In many ways, the internet is just a mirror of our real world. It has it's safe places, areas you would hang out with your friends. But it's also full of people who don't have you - or your child's - best interests at heart. It's a difficult topic, but all of the bullying, abuse, and sexual exploitation of children in the real world can be found online too.

Bullying at school follows a child home on their phone and in their games. Child groomers pretend to be children and work to build a foundation of trust as a gateway to abuse. Social media shows an idealised version of what people should be. Inappropriate content is all too easy to access. There are just too many pitfalls that your child can fall into.

The internet is constantly evolving. People used to only be able to hide behind an anonymous name, but now they can pretend to be an entirely different person. Look at deepfaking; people are able to take a celebrity's face and put it onto any video, making it look as if they really said or did those things. It's all fun and games when it's a joke, but how long will it be until it's happening to the general public? Or used to deceive us?

In a world of trolls, catfish, fake accounts, and Facetune, the internet is a dangerous place for everyone not on their guard. And children are the most at threat.

Getting rid of the internet is too unrealistic today. In the '90s or early 2000s, as it was just picking up steam, you could arguably live in an internet-free household. But now it's too intertwined with our daily lives. It's how we consume entertainment, communicate with friends and family, and even do our jobs. And learning computer literacy is a vital skill for anyone to have. So that solution isn't possible.

It's made all the more difficult, though, by the sheer number of devices in our household that can access the internet. It isn't just computers. Phones, tablets, game consoles, and even fridges can connect to the world wide web. That's a lot of opportunities for your child to see or hear something they shouldn't. The effect that has on your child will vary depending on how naturally resilient they are, but it's never good for any child. Unfortunately, we've all heard tragic stories of children who take their lives due to cyberbullying. Those are the worst-case scenarios; there will be thousands more children who become addicted to games, the internet, or even pornography.

Thankfully, big technology companies have realised this, and most devices and services have some level of parental control that allows you to block out the most inappropriate content. There's also a variety of tools you can use to add further restrictions. We've even made one ourselves. Wardwiz Essentials Plus available for laptop, tablet Android and IOS.

But this is only half the battle.

At WardWiz, all of our products feature parental controls as standard. We're dedicated to providing exactly what parents need. That's why we spent 18 months talking to children's charities and parent support groups to get to the heart of the problem. What we found is that parental controls will only get you so far; it's up to us as parents to bridge the gap.

There are a terrifying number of parents who leave their child to their own devices. They don't think to check what their child is watching, playing, or saying to someone else. Even with parental controls on, you can't prevent them from seeing everything. You have to be there to guide them.

Notice we said "guide" and not "judge". Something you need to remember is your child is a victim in most scenarios. You can't approach this from a confrontational angle. You have to work with your child, coming at them with mutual respect and letting them know that this is your fight together.

This is your handbook for keeping your children safe.

They have to feel comfortable sharing their online life with you and talking to you about matters that make them feel uncomfortable. Yes, this may get more awkward as they get older; no teenager is going to want you to know all the details of their social life as they're finding their place in the world. But they need to know that you're their ally who will always help them. If they come across someone who doesn't seem right, they need to tell you. That can't happen if they don't trust you. There are times where you'll be the villain. To them, you'll be the worst person in the world. There's no stopping that sometimes. That's why it's all the more important to keep your cool, stay level-headed, and explain to them everything you can.

As we discuss everything you need to know about parental controls, keep that message at the forefront of your mind. This is your handbook for keeping your children safe. It isn't here to help you catch them out or discipline them. There are lessons within that you have to take to your child and work with them on. This includes technological literacy, critical thinking skills to notice when something isn't above board, and general online etiquette.

And we hope it will be just as educational for you. Even if you aren't the most proficient with technology, our step-by-step guides will leave you confident that you can master these parental control features. We're with you along that journey and will always be here to help.

We hope this book is everything you need it to be. The information in this book is correct at the time of writing, but the internet is forever changing. Companies may change how their parental controls are accessed. If you ever have any questions, we're easy to reach at wardwiz.co.uk. While you're there, you can also subscribe for further updates and tips to help you guide your child in the right direction online. So without further ado, let's dive in...

An introduction to parental controls

It can be shocking to see just how much is actually involved in trying to protect children from harm online. Unfortunately, there's no silver bullet. But one tool you have available to you is parental controls.

Parental controls are settings that can be applied on digital devices such as smartphones, tablets, gaming consoles, computers, smart TVs, games, and apps. They are absolutely essential in the fight to protect children from harmful or inappropriate content and cyberbullying.

It requires you to sit down and review all of the digital access points your child has access to, then look at each individual game and app they use. Once you lay all of this out, you can see exactly what level of protection your child needs.

It's crucial to note that not every family will have the same requirements. We feel it's far more important for parents to fully comprehend how psychology and consumerism drive so much of our online activity. Having this understanding allows parents to better assess their own children's online activity and exposure. When setting up parental controls, it's advisable to set them higher than you might think necessary, especially when it comes to younger children.

Make no mistake, parental controls are not a 'set and forget' tool. Parents have to be constantly vigilant as children can often easily bypass parental controls. A simple YouTube search will show them how to circumvent even the best measures put in place. So we must be conscious that parental controls are not a substitute for parenting. You have to be an active participant in your child's online life, restricting, monitoring, and educating a child as they grow. This helps them develop a resilience to the darker elements of the online world.

The parental controls will create a barrier to protect children from exposure to harmful content and people online, but we need to be mindful that no parental control or filter is 100% secure. Inevitably, exposure does occur; this is why having an open level of communication with your child is key, as they can let you know if such an incident occurs. We strongly discourage parents from shouting at a child if you discover they've accessed inappropriate content. Also, don't take the device from the child afterwards as a punishment. In our experience, having spoken to literally thousands of children, suggests those punished in this way are exceptionally reluctant to inform their parents of any further exposure. Parents and children have to be on the same page if you want to have open and honest conversations about online experiences. Children are at a serious disadvantage and are considerably more vulnerable online if they can't talk to their parents about it.

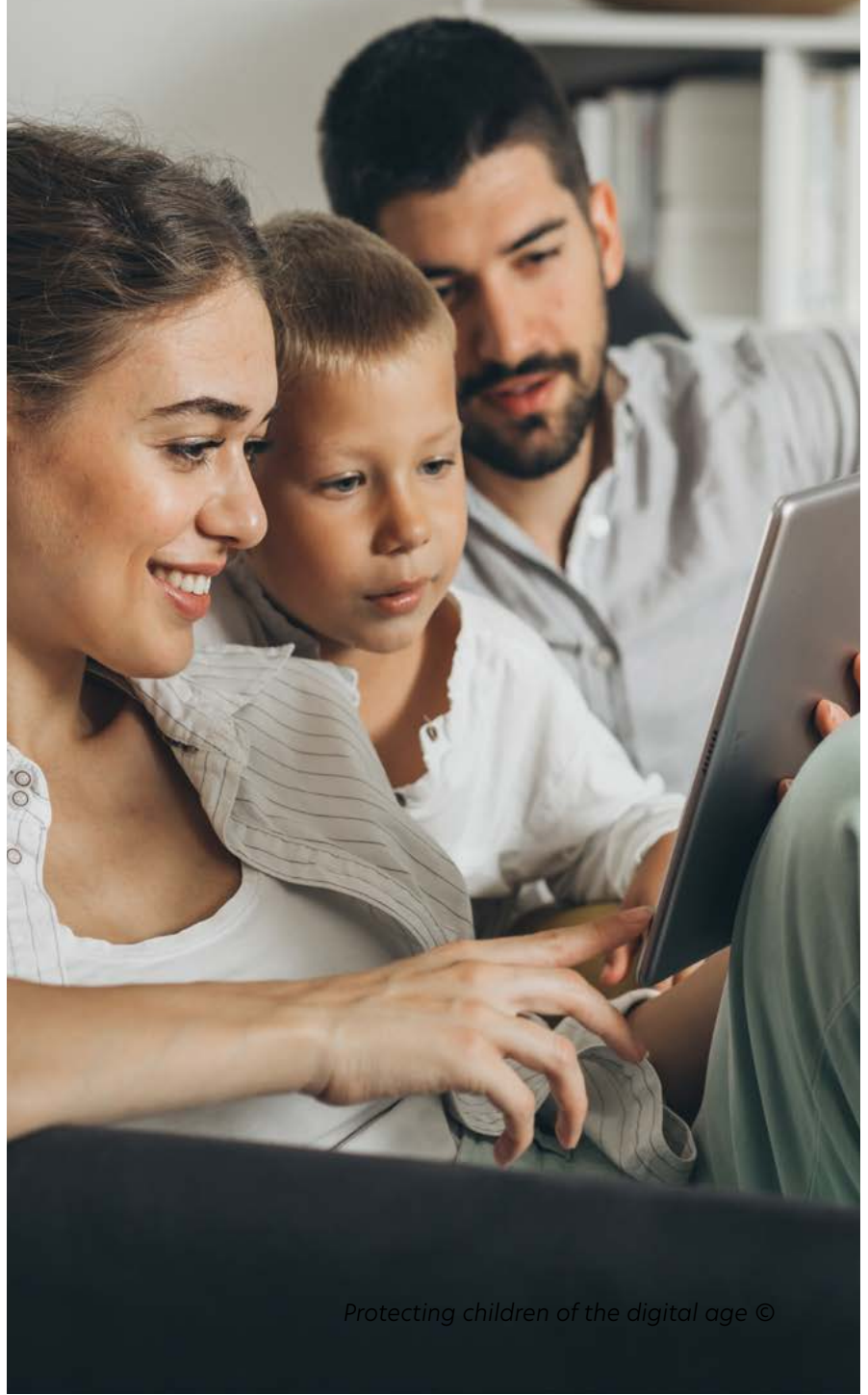
With so much information in this book, it might seem easy to become overwhelmed. But don't worry. This guide has been designed to take slowly and plan out the best route for you and your family over time. Everything is clearly segmented, allowing you to jump back and forth as you please - whatever works for your unique situation. If you have any more questions or you feel you have a situation we haven't covered, just let us know by emailing us at PC@wardwiz.com.

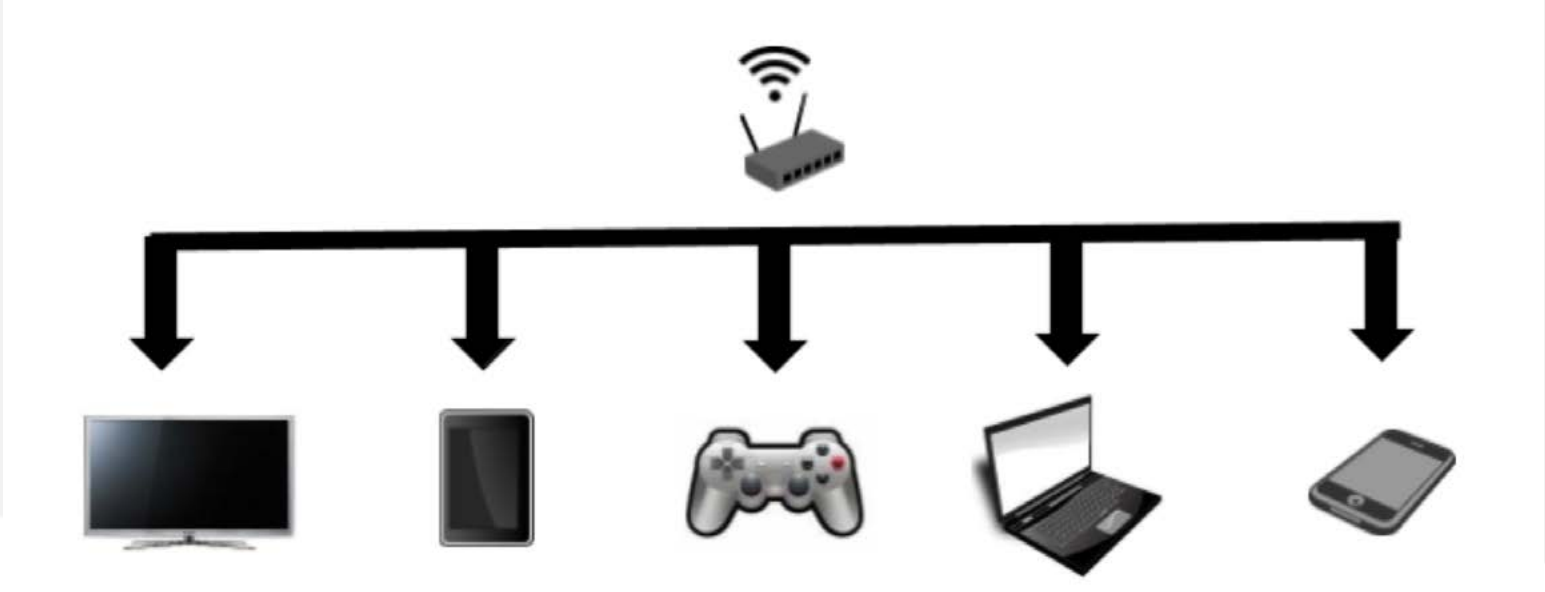
How to use the parental control guide

Welcome to the ultimate parental control guide. We suggest you take the following steps before you begin setting up parental controls on any device. This will save you a huge amount of time and show you what the most appropriate requirements are for your family.

Creating your family online safety roadmap
A roadmap will plot the best route in helping you to establish what devices you have, what access your children have to the online world through these devices, and what type of content is available. There are two options to consider at this stage. Can your Wi-Fi router be used to restrict and monitor content? This may save you some time. If not, does the device have its own parental controls or do you need another application or parental control product to restrict access?

To find out what settings are available through your Wi-Fi router, a quick search online with the product code should yield some useful results. Changing these settings will likely mean having to log into the router's IP address (it's unique digital address found on the back of the router) on your computer, tablet, or phone.





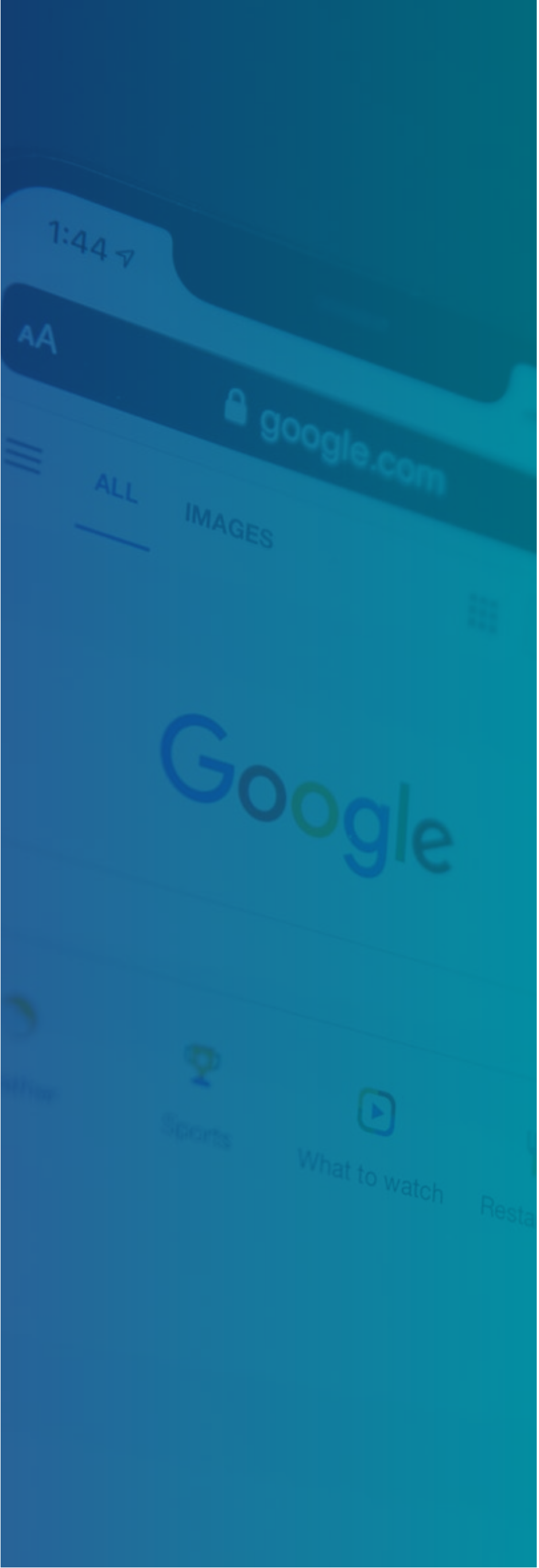
Step 1 - Make a list of the current online access points in the home

The average home with two parents and two children under 12 years of age can have as many as 20 digital devices. Think about it, both parents will likely have a smartphone each and a PC or laptop, possibly a tablet too. Then you might have a smart TV in the home - potentially multiple - that connects to a Sky box. Both parents and the children will possibly have access to a streaming service like Netflix, Disney+, or Amazon Prime. Then the child themselves will usually have a gaming console of some description, their own tablet (such as an iPad), and depending on the age of their child, a smartphone. And then there are all of the individual apps and games - both online and offline - that your children use and play.

Step one is to compile a list of all of the devices in the home where a child can access to the internet or is using the internet as a delivery system to access content. There are a number of considerations when making this list. Is there more than one user of the device? What is the device used for? What content can be accessed on the device? Can the device be used outside of the home? If it can, then simply restricting content at the Wi-Fi router is not going to prevent that child from accessing unrestricted or monitored content.

When you've finished your list, you can more easily see which devices can be restricted through your Wi-Fi router. Then there will be others that need you to dive into the settings yourself. And those that may need an extra service. Or it could be a combination of any of those. Whichever path you choose, it will take a little time to plan out.

It's important to go through this process at your own pace. It doesn't all have to be set up in one day, so take your time and get it right. No need to cover the same ground twice if you don't need to. To start with, why not map out some of the main devices in the table on the next page?



Step 2 - Make a list of all of the online platforms that are currently being used

It isn't enough to list just the devices. To use any smartphone, tablet, game console, or media streaming service, a user account is required, which means your child's data is going somewhere. There are a variety of options available on existing platforms, which do have various levels of parental control settings. Some Wi-Fi routers will assist by blocking content at source. However, they can be ineffective when it comes to the likes of streaming content. As we cover all the platforms that you're likely to come across in this book, once you have your list, you can find the ones that are relevant to you, with helpful tips on how to set up the parental controls for each one. Note that some platforms require extra services, such as Apple iOS ScreenTime or Google Family Link, and potentially even a subscription-based parental control solution.

Often when a platform requires a separate account for your child, it means they have a safer, child-appropriate setting. Where possible, ensure they have their own account and avoid using your device. If you do allow your child to use your device, they should have their own account that doesn't have administrator privileges, otherwise you're handing them an access-all-areas backstage pass. Many adults find it difficult to identify potentially harmful communications, links, and websites, so the task is even more difficult for children. A child using a device that contains sensitive personal data may inadvertently put the security of the device at risk by installing something they shouldn't or opening a suspicious link.

Child's name & age	Device type	Is a parent account set up required?	What can be accessed?	What restrictions are available?	Are other parental controls required?	Is there protection on multiple platforms/devices?

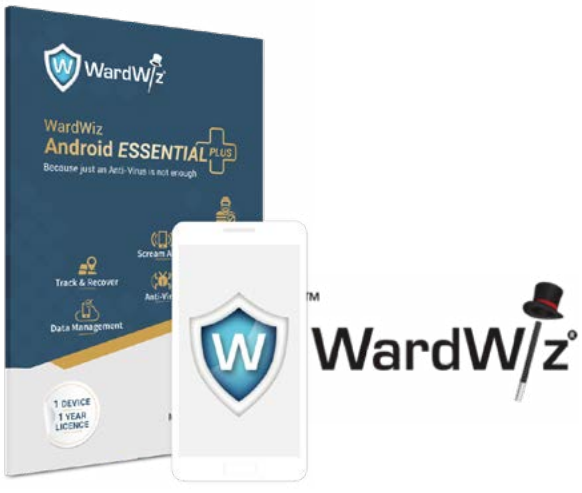
Step 3 - Set out the specific requirements for each child based on their age

It's possible to set different age restrictions on some platforms dependent on the age of each user. To do this, each child will inevitably have to have their own account. You might find this task arduous if you have a lot of children. It might be best to set the setting under PG, 15, and 18 as these are usually the three catchall age ranges. Note, however, that content available with an age rating of 15 can contain content which up to a few years ago would have been considered only suitable for a much older audience.

It helps if you base your decision on your own children and their level of maturity, as opposed to an age rating. Some children can be a little more or less mature than their age. Certainly, for children under 11 years of age, every attempt should be made to maximise the restrictions on all content available to them. We don't get to take back anything that a child is exposed to by accident or design, so please make every effort to ensure every measure has been taken to protect them.

Step 4 - Consider the use of parental control devices and applications

We've mentioned external parental control options a few times now. So we've set out a few options that might be worth looking into. Some products are a little more expensive than others, so it's worth having a look through them to find the one that best fits your family.



WardWiz Android Essentials for mobile, iOS Essentials for Apple mobile, and Essentials Plus for laptops and tablets. These products come with a range of features. They can be used on mobiles, laptops, and tablets.

Features include:

+ Full antivirus protection with Android Essentials and Essentials Plus.
+ Set daily time limits for how much children can access the internet.
+ Lock the App Store to ensure all downloads are pre-agreed by the parent.
+ Block inappropriate keyword searches.
+ Track the child and set a location geofence which will send an alert if they leave this area. For example, if they move over 300m from the cinema or a friend's house, you can receive an alert.

This option is available for as little as £1 a month. Use discount code PC50 to receive a 50% discount on any WardWiz products. Download links are available on the site.

Website: www.wardwiz.co.uk

iKydz

This product allows parents to monitor and restrict their children's online activity both inside and outside the home. It can be used on mobile phones, tablets, laptops, smart TVs, gaming consoles, and more, which can all be controlled from the palm of your hand anywhere in the world.

Features include:

+ Block adult content.
+ Schedule time spent online.
+ Block or limit access to social media.
+ Block gaming or gambling sites.
+ Filter content on YouTube.
+ Monitor what your children's devices are accessing.
+ Cutting internet access on all devices from one push of the Meal Time button.

This option is slightly more expensive, setting you back £5.99 a month.

Website: https://www.ikydz.com/

Google Family Link

It's highly recommended that parents make use of Google Family Link (or Apple Screen Time for Apple devices). Both are free applications and offer an extensive variety of parental controls. At the very least, we would strongly advise parents you use these, but you need to be aware that this is not a catchall, so it will have to be used in conjunction with other parental controls.

Features include:

+ View their app activity.
+ Manage their apps, approve or block apps.
+ Manage in-app purchases.
+ View teacher-recommended apps on Android that you can add directly to their device.
+ Keep an eye on screen time.
+ Set time limits.
+ Remotely lock their device.
+ See where they are.

Google Play Store: https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylink

Once you've recorded all the devices and platforms your child uses, take some time to research the above protection to see what feels best for your needs. To protect a child fully from harm, multiple parental controls are required. So, for example, an average home with Sky, Netflix, a single tablet, and an iPhone will require a parent to set up parental controls on Sky and a child's profile on Netflix. In this scenario, you might consider taking the less expensive route of installing Google Family Link on the tablet and Screen Time on the iPhone.

We're not here to sugar coat it. Creating a safe online space takes time and can feel exceptionally frustrating, especially for parents who are not technology literate. But it doesn't have to feel overwhelming. By taking these simple steps, you can take the complication out of internet safety and feel comfortable you understand the best steps to take.

For smartphones, tablets, iPads, gaming consoles, and streaming services, the most important factor to remember is to have a supervisor account, which will be your own, and then the child's account, which is used to set the restrictions and monitor applications and settings. It's possible to set up multiple accounts for children on many platforms and to have a large variety of restrictions set up on each one according to the needs of the user.

Step 5 - Review and risk assess

We've looked at the platforms and devices that your child uses, and now we want to consider the possible avenues of risk to your child in the home. This will include ensuring you know who the child is in contact with online across all platforms, games, and apps. If a potential risk is there, have a plan in place to deal with it. Keep in mind where the devices are in the home and your ability to monitor them. Think about switching off the Wi-Fi at night or use screen-time management features. Replace a digital device currently being used as an alarm clock with an actual alarm clock. Create a central charging station in the home for all devices. These are simple changes you can put in place that better allow you to monitor what's going on.

There are far more considerations than most people would care to give credit for when trying to protect children from online harm. Make it your business to regularly ask your children how they are getting on online. If you don't ask, you might never find out. Sit down regularly and see what apps, games, and platforms are being used. Download them yourself and try to get a feel for them. Or ask your child to take you through how they use it. The more collaboration and communication you have, the better prepared you're going to be in the event something goes wrong. Unfortunately, there's plenty that can go wrong.

Step 6 - Getting started: prepare to be undermined

Internet safety is not a sprint; it's a marathon. And an unending one at that, as digital devices, apps, and games usually only have a certain shelf life. Just when you get on top of the most popular ones, another inevitably comes along to take its place, so it's worth creating positive habits to reinforce positive internet use now, to maintain

A big part of internet safety is education through communication and not making your child feel like they're being punished.

---

a safe online space for them.

As a parent, you're in the right place. If you've been filling out these sections as you go, you've already done the hardest part by taking the first step. You'll quickly notice that across a lot of the platforms, the parental controls are both similar and straight-forward to use. Rome wasn't built in a day, and it will certainly take more than a day to work your way through all of the different online avenues that need to be childproofed. If you're still struggling, it might help to work through this with a family member or friend - someone who's a little more technology literate than you. Failing that, you can always message us on the WardWiz Facebook page if you're stuck and we'll do our best to help you.

As well as being technically prepared, we want to mentally prepare you too. A big part of internet safety is education through communication and not making your child feel like they're being punished. If you make a fuss about setting up parental controls, you create a battle. You'll start to find your child will attempt to undermine all of your attempts to protect them as they don't understand why you're doing what you're doing. Let's be honest, we didn't grow up as children of the digital era, but if the shoe was on the other foot, we'd have tried to do the same ourselves. Treat them as equals and rationally explain why it's so important to be protected online. Ruling with an iron fist will only push them to hide even more, which can cause problems later on. While open communication is essential, children also have to be aware there are consequences if they're found to be breaching any of the house rules relating to online safety measures.

To overcome this, try using a social media contract. We've put one together to get you started. There's a section for you to write in whatever punishment you deem appropriate for a breach of contract. You could also include positive rewards to suit your family dynamic or what you as the parent will do to protect their boundaries (within reason) so it feels like a fair agreement. Once you've determined the rules, you can both sign it and agree to abide by the terms.

Children of the Digital Age

Social Media Contract for Kids

Setting up

- ◯ I will always ask my parents' permission before joining a Social Media Site
- ◯ I will allow my parents to set my privacy settings and parental controls on all my accounts
- ◯ I will give my parents the passwords for all my social media accounts
- ◯ I will **NOT** give my passwords to anyone other than my parents
- ◯ I will **NOT** change my passwords without my parents' permission
- ◯ I will **NOT** set up any private or secret Social Media accounts

Sharing

- ◯ I will **NOT** share any of my Personal Information without my parents' permission
- ◯ I will **NOT** post or share pictures of myself without my parents' permission
- ◯ I will **NOT** post pictures of family or friends without my parents' permission
- ◯ I will **NOT** share any offensive or inappropriate images, videos, comments or content
- ◯ I understand that I am responsible for anything I post or share online

Content

- ◯ I will **NOT** ever meet anyone who I have only met through Social Media
- ◯ I will **NOT** engage in online bullying including unkind comments on the posts or comments of others
- ◯ I will always let my parents know if I am experiencing any form of online bullying
- ◯ I will agree to the time limits that my parents set for me for being online
- ◯ I will **NOT** allow my school work to suffer because of spending time online

Consequences

I understand that if I break any of the above my parents may

1 _____

2 _____

I _____ understand that my parents have set these consequences to protect me and keep me safe when I am online.

Some advice to parents about social media

Social media has taken the world by storm. Very few young people have managed to avoid the lure of its siren call. For every person who has opened an account and found it to be a positive experience, there's someone else who was dismayed to find out just how negative it can be.

The landscape of varying platforms is vast. Some of the more popular choices among young users are Instagram, Snapchat, TikTok, Twitter, Discord, Twitch, and WhatsApp. Each greatly different from the others. From speaking with teens about social media sites, Facebook is only for oldies such as ourselves now. But while it might look like Facebook is dying a slow death, Mr Zuckerberg won't be troubled in the least - he also owns Instagram and WhatsApp, by far the two most commonly used platforms among users both young and old.

Before we jump into the topic, it would be unfair not to acknowledge some of the positive aspects of social media. It's a great way to stay in contact with friends and family. It can be an incredible way to support causes and stay informed about what's happening in the world. It's also a platform that can be used to develop your own sense of identity. A way to be creative and be an inspiration to others. It can be used as an education tool or to encourage personal and business growth. Push your message on a truly global platform. Used in the right way, it can achieve so much.

However, our concern - and yours as a parent - are the negative ones, particularly among teens. Unfortunately, and being very realistic, to list all the negatives is far beyond the remit of this book, so we will just concentrate on the immediate dangers faced by children.

To understand why, we need to look at what social media is, how it ensures user engagement, and how it influences our behaviour. We can learn a lot by simply taking a step back in time. Back to when you initially created your own account. What drove you to become part of a global social network? In all likelihood, you'll have heard about the platform through the grapevine, with plenty of people you know raving about how good it is. There was possibly a little bit of curiosity. A realisation of how user friendly it was, followed by wonder at how easy it is to communicate with people far and wide.

Without any concerns for privacy, or realising how many people might access your content, you began sharing and commenting. Your posts then received attention from others, who were also sharing content which captured your attention. Suddenly, as the number of likes and comments started to flood in, all the positive attention became addictive. So you post even more personal and private content. You possibly didn't even notice the psychological subversive methods that were used to get you hooked. So the question to ask now is would you do it all over again?

Social media became a very useful tool for countless people all over the world. However, as more and more people joined, the dark side started to become more apparent. We realised how little thought was given to the privacy of a user's personal information, especially children. Now, we're aware of how it's used as a method of accessing images of them. A tool used by online sexual predators to make contact with them. An awareness of a darker side of social media brought with it a new terrifying reality. Not only are children vulnerable, teens and adults are too. Cyberbullying and trolling became more prevalent, while romance scams and other criminal activity also began to take hold. The eventual manipulation of voters during the 2016 American presidential election in the Cambridge Analytica scandal is the ultimate sign of just how dangerous social media has become.

Today, it's often used as a way to define who we are. There's this idea that, if you aren't on social media, are you even living? Of course that's ridiculous, but that addictive need to be liked and acknowledged is hard to break for some. The online world allows you to be whoever you want to be. Both in the sense of putting on a facade and pretending to be something you're not, and literally pretending to be someone you're not. In those early days of social media, people thought this ability to interact online would be a huge benefit to the shier people among us. The term "the poor will get richer" was frequently used as a means to describe how even the most inhibited could become very active without experiencing the insecurities felt in the real world.

To a degree, the poor did become richer. But the rich also became richer. Extroverts thrived on social media. But this brought about new problems. Popularity online became a status symbol which extended into the real world. It's like Lord of the Flies - the social media landscape became a battleground to put down the more vulnerable or less popular kids. It became a place to target and bully others. This has led to tragic circumstances for many young people and their families.

Another serious consideration is whether it's an image sharing platform, such as Instagram or Snapchat. There's a real danger for young people to compare themselves to other people. It's always going to be a fruitless exercise. With so many filter apps available, it's all too easy for people to change how they look, even beyond recognition. This can lead to self-confidence and self-esteem issues, and even social anxiety. In the worst cases, it can lead to self-harm and, unfortunately, to some young people attempting - sometimes successfully - to take their own lives.

Beyond that, children can interact with anyone they please. In a world where you can be anyone you want, what happens if a child develops troubling interests? It doesn't really matter what a person believes or how misguided their ideas are, you'll always find people who think the same way online. If this group holds beliefs which are harmful, dangerous, or extremely radical, it's all too easy to be dragged into that spiral of hate. We've seen many cases where seemingly naive and innocent young people get swept away by radicalised communities. This is one of the reasons why it's incredibly important to know who your child is interacting with online.

There are further dangers with online predators who gather in droves on platforms popular with children. These people are very successful in developing trust with kids. While your child might believe it's another innocent person their age, it can quickly escalate to an adult having full control over your child, demanding they fulfil the sexual demands of the online predator either online or in-person. With live streaming and image sharing now easily accessible, it's an unparalleled opportunity for predators to sexually exploit children without actually meeting. The currency of online sex offenders are images and video that nobody else have. It's now easier than ever to have this content created on demand and share it with others. The UK cybercrime prevention team reports that over 75% of child pornographic images are self-created. But it becomes a cycle that keeps the young person trapped. Either they like the attention too much or they're blackmailed. And in the worst cases, the child themselves might be traded.

This issue is not made any easier thanks to the ability to mask your online identity. It's often said that only the stupid ones get caught. This may be true. However, if we consider that, on average, an offender can accumulate as many as 400 victims each before being caught, that's a considerable number of children being harmed. What's more terrifying is the number of individuals who genuinely see no harm in what they're doing. Individuals who believe they're just genetically attracted to children. They're merely expressing their love for the child and having an intimate relationship with them. It's society that doesn't understand them. At least, that's what they try to tell you. At any given moment, there are an estimated 500,000 online sexual predators active online. Parents really need to be cognizant of this when their children have unsupervised access. This isn't an attempt to scare you or convince you that the online world is bad. It's merely just a way to show how easy it is for something to go wrong when we don't pay attention, and why keeping that open communication is key.

It doesn't help that, regardless of the platform, all social media companies use similar techniques and ever-advancing algorithms to ensure user engagement, in an attempt to be the dominant player. And they'll use whatever content they can to keep eyes glued to the screen. This can potentially expose children to harmful content they're too young to see, much of it not age-gated (i.e. only available to people above a certain age).

The algorithms decide which content to put front and centre, and it's usually whichever gets more of a reaction. More likes, more comments, more shares. This, in a way, removes your own free will, as the platform is deciding for you what it believes is important, based on your activity. We then have the matter of an echo chamber.

The algorithms decide which content to put front and centre, and it's usually whichever gets more of a reaction.

Again, ideas, beliefs, and concepts can be manipulated by the platform through the comments, content, and activity of others it chooses to show you. A misguided belief can be strongly reinforced when only the particular type of content from others is displayed on your newsfeed. Eventually, this can be seriously detrimental to a person's ability of critical thinking, as the platform is essentially removing ideas or concepts that would challenge your own ideas or beliefs.

We mentioned it before, but the Cambridge Analytica scandal is a great proof of concept. Here you had a company analysing people's personalities and activities, and specifically targeting them with content that would influence their choice during the election of Donald Trump and the Brexit campaign. It knew what you wanted to hear and pushed whatever it felt it needed to - even if it was fake - to sway opinions. That isn't to say it affected everyone's decision of how they voted, but it did stop people from thinking for themselves and challenging their ideas. If we can't expect every adult to do this, how can we expect it of our children?

The social media validation feedback loop, a long but aptly titled term, describes the psychological process that takes place when we share content that others like or comment on, while we do the same on their accounts. This is a mischievous and subtle effect that takes hold of us, without us even realising it's happened. The more likes or comments our post has, the more popular it becomes. And the more this happens, the more we want it to happen again.

Sean Parker, former president of Facebook in 2017, said: "These tools rip apart the social fabric of what society has created. Facebook knew very well about how checking a user's 'likes' and 'loves' would provide a dopamine hit as part of the social validation feedback loop that our brains crave. The hook cycle starts with a trigger, the action phase, in anticipation of a reward that will make you feel good. When our smartphones alert us to any kind of message, they prompt us to respond immediately in anticipation of that reward."

Social validation feedback loops can be identified in a number of ways. Have you ever felt compelled to like or comment on a close friend's content, even though you don't actually like it? It's almost as if there's this feeling of obligation. If you ignore a post, is there a completely irrational fear of being asked why you didn't like it? Or if a small number of friends or followers are constantly acknowledging your posts, do you feel obliged to reciprocate on their posts? Have you ever felt an urgent need to share a post immediately, after being positively or negatively emotionally impacted by a post? If the answer is yes to any of these questions, then you may be caught up in social validation feedback loops.

"Facebook knew very well about how checking a user's 'likes' and 'loves' would provide a dopamine hit as part of the social validation..."

Another serious consideration is the friend and follower dilemma. Since the arrival of Facebook - which has outlasted several other platforms, such as the long defunct Bebo and MySpace - the term 'friend' has lost its real meaning. The term has been diminished enormously; an acquaintance of an acquaintance can now be our 'friend'. We've met children with literally thousands or even tens of thousands of friends. When asked if they know them all, of course they say no. But, like anything else with social media, seeing that number go up is addictive.

We use the 'rule of touch' to teach children the difference between a stranger, an acquaintance, and an actual friend. It's simple - the child must be able to state when and where they were able to touch the person on the shoulder. If they can't, then this is not a friend. We like the golden rule that only people who meet this criteria can be engaged online.

If they already have accounts, sit down with them and go through their friends and followers. Remove any people who can't pass the rule of touch. We've found this to be an excellent tool for parents and children alike. What has surprised many parents is how fast children take to this simple rule. Often, children - and even adults - feel obliged to accept new requests from friends of friends. Just like the real world, a stranger is a stranger is a stranger. If you don't genuinely know them, you shouldn't give them access to you or your account.

You'll also have to explain that not every account is genuine. Many are created to take advantage of both adults and children. It can be helpful for young people to know that adults too can be targeted by people who may not have their best interests at heart. Asking a person in the real world if they sent a request is a momentary positive action that may save a lot of distress if it isn't genuine.

There are other serious issues when it comes to social media - get ready for an extremely long list: the permanence of content, privacy, data protection, data breaches, the age of digital consent, image harvesting, image manipulation, image abuse, online reputation, false accounts, hacked accounts, clickbaiting, like harvesting, malware, cyberbullying, online hate and racism, graphic content, trolling, flaming, catfishing, identity theft, scams, fraud, honeypots, online exploitation, online sexual exploitation, and many more.

That's how much can go wrong. And all of them are equally prevalent online. While social media platforms are making every effort to address all of these issues, they're a long way off making platforms safe and secure enough for children. This is why we strongly recommend that no child under the age of 13 is ever given access to social media, and only allowed access at 13 if they're fully aware of all the dangers and agree to rules of use and constant checks by a responsible trusted adult, who is mature enough to use it and does so in full cooperation with a parent or guardian. Unless they meet that specific criteria, under no circumstances should they have an account.

A word on privacy concerns and BlueStacks

Certain apps and services require you to have an account of your own to use some of the parental control features. If you don't feel comfortable downloading certain apps on your own device, whether it's due to privacy or security concerns, there are ways around this.

An alternative is to download and install a program called BlueStacks on your PC. This allows you to install a virtual Android operating system on your computer. It mimics what you would find on an Android phone, allowing you to download apps and use them within this virtual field.

You can find the latest version here: https://www.bluestacks.com/

Once you've installed it, open it up and select the Google Play Store icon that's on the home screen. You'll be prompted to sign in with a Google account. You may use an existing account or create a new one just for the purpose of creating parental control accounts.

When you log in, you can use the Google Play Store as if it were on an Android device. The apps you install will also appear as they would on an Android device.

1

Popular apps

Facebook

Facebook is one of - if not the - biggest social media networks out there. While it might not be as popular with the younger crowd as it once was, your child still might want to be part of the action.

We'll start by saying that no child under the age of 13 should be permitted to create their own Facebook account. There are no built-in parental controls available on the platform. For teens, it's best to manage the general account settings to ensure profiles are as protected as possible. Our advice is to ensure you have full access to your child's account by sharing it and having the application installed on your device. This allows you to see what content they're looking at, who they're talking to, any new friend requests, and any messages they're sending and - more importantly - receiving.

You also need to be aware of all the personal data Facebook collects and the potential for harm in the future. Society as a whole is still coming to terms with the negative implications of unfettered harvesting of personal information, its sale to third parties, and its subsequent use. Please take a moment to read the terms and conditions before downloading any application.

If you do end up creating an account for your child here's a more detailed look at how to make Facebook safer.

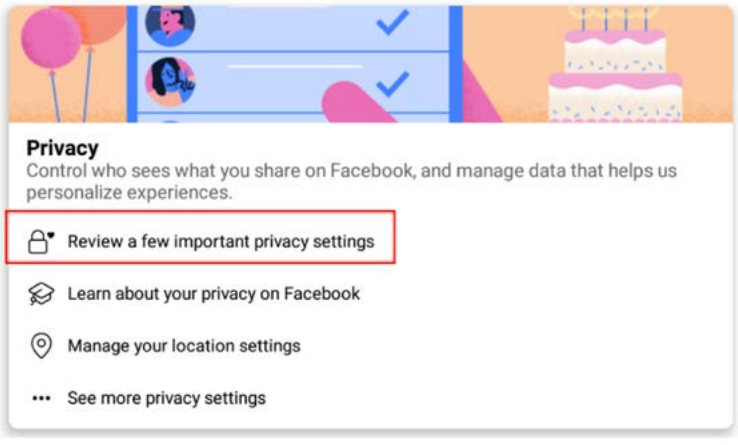
Restrictions available:

+ Ad preferences
+ Inappropriate content
+ Online chat
+ Privacy
+ Limit social network posts and contacts
+ Prevent identity theft

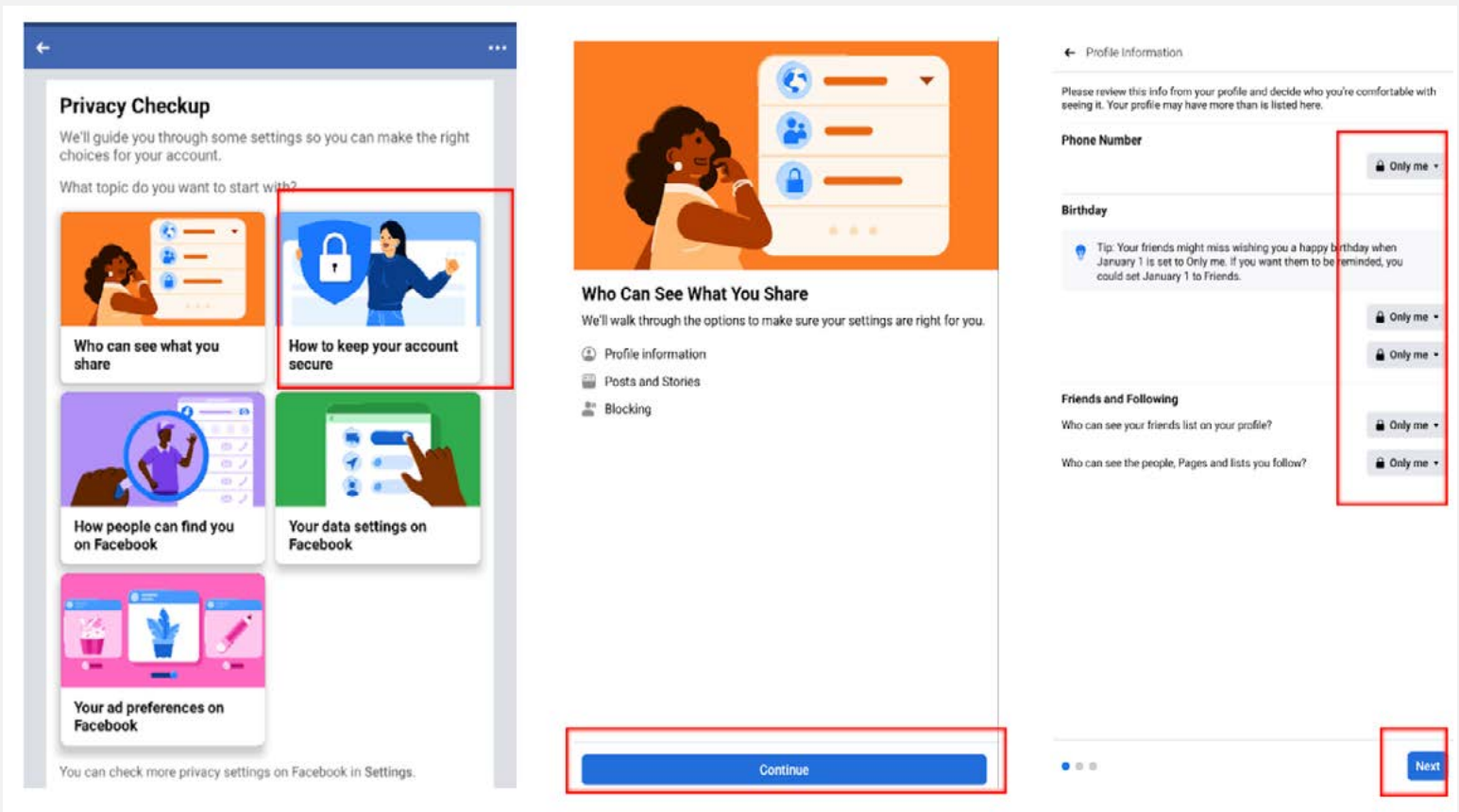
Let's take a more detailed look at how to set up your child's Facebook account and what you can do.

Setting up the privacy and security settings

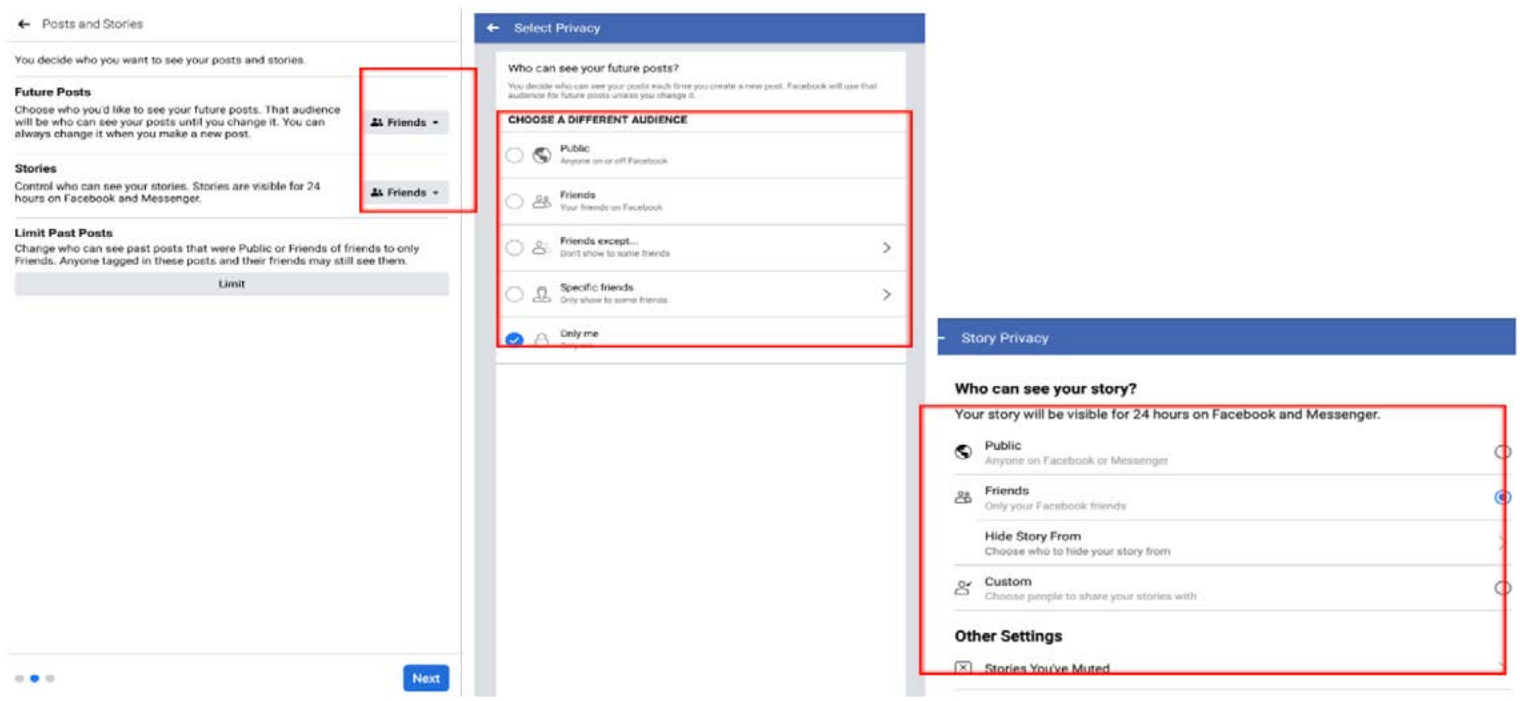
+ Log in to the Facebook account using the **email address** and **password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and **select settings and privacy**.
+ Now select the **privacy shortcut** option.



+ A menu will appear on screen which has a variety of different settings to review. It's important to take time to go through each of the individual sections to ensure the account is secured to meet the needs of your child. For now, however, select **'review a few important privacy settings'.**



+ Select **who can see what you share**. This menu allows you to restrict access to your personal information, posts, and stories. There's also an option to block specific Facebook accounts.
+ Select **continue** on the page that opens.
+ It's strongly advised that no personal information should be accessible to anyone on this platform. Often, people overshare, which could be used to target an individual through social engineering ploys or leave the account holder vulnerable to identity theft.
+ By setting all options to only me, no personal information is available to other platform users.
+ Once finished, select **next**.

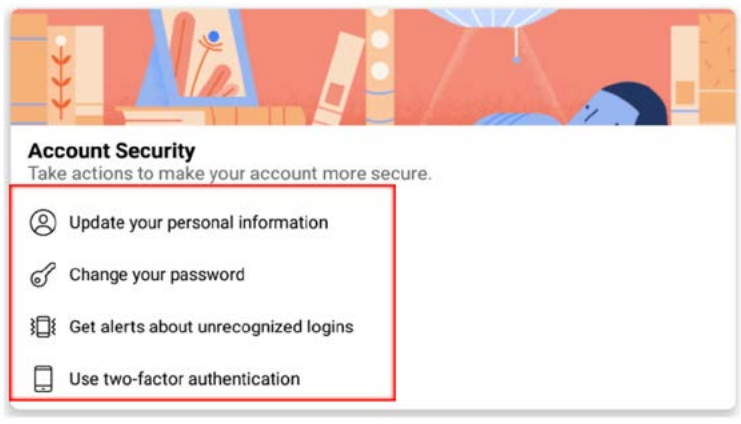


+ Select the **posts and stories** option.
+ When it opens, select **future posts**. It's important to limit who will have access to this content as countless people have done incredible harm to their online reputation by posting inappropriate

content. Review this carefully with your child or teen and discuss the implications for posting or sharing negative or harmful content.

+ Return to the menu and select **who can see your story**. Again, serious consideration is required regarding who can access the content shared on the platform. The more restricted it is, the better. However, parents need to remember that a post shared on the platform may be reshared by other users.

+ If your child has had an account and has been active on the platform for some time, they may already have content which would reflect negatively upon them. By selecting the limit option, all previous posts to date will be limited in regards to who can access them. Once this option is selected, a user will have to go back through any post that has been shared to change it manually if they wish to make it available to other users who are outside of the limit being set.

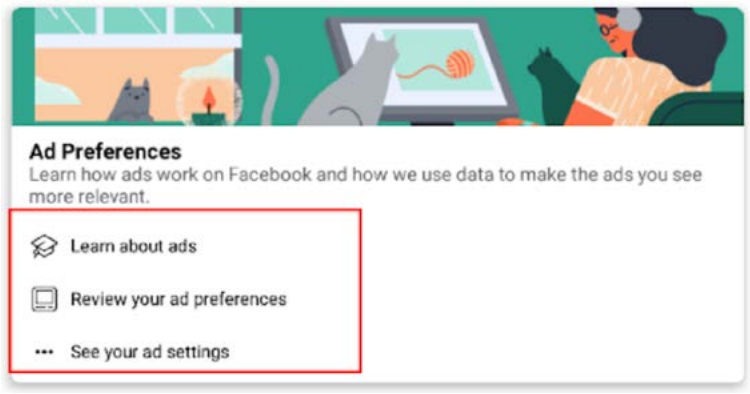


Setting up the security settings

+ Log in to the Facebook account using the **email address and password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and select **settings and privacy**.
+ Now select the **privacy shortcut** option.

This menu allows you to:

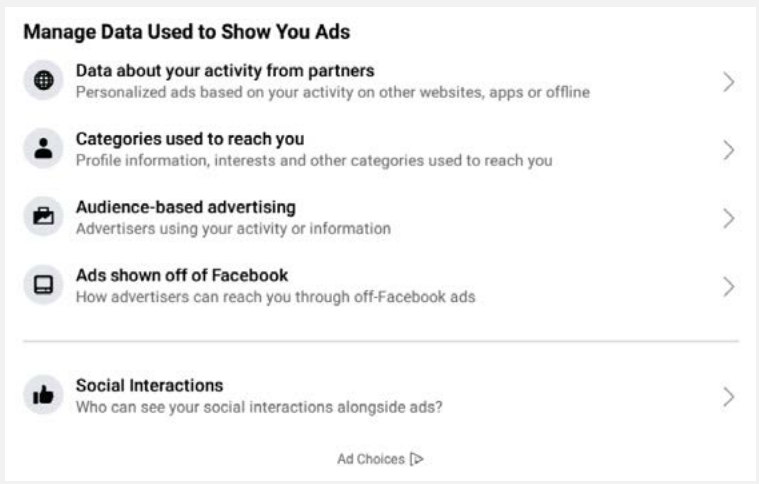
+ Update your personal information to change your name, contact info, or identity confirmation.
+ Manage your account and deactivate.
+ Get alerts about unrecognised logins. Ensure this option is activated to ensure that you are immediately made aware should someone other than you attempt to, or be successful in, logging in to your account.
+ Use two-factor authentication. It's strongly advised that you enable this option. Also, we would advise against using a mobile phone number as the second form of authentication. Instead, use an authentication app.



Setting up ad preferences

+ Log in to the Facebook account using the **email address and password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and select **settings and privacy**.
+ Now select the **privacy shortcut** option.
+ Select ad preferences.
+ Select the appropriate settings under each category:
    + Learn about ads
        + What data is used
        + Your controls
        + Why you see a particular ad
        + FAQ
    + Ad preferences
        + Advertisers
        + Ad topics
        + Ad settings

+ Select **ad settings** to manage what your child sees.

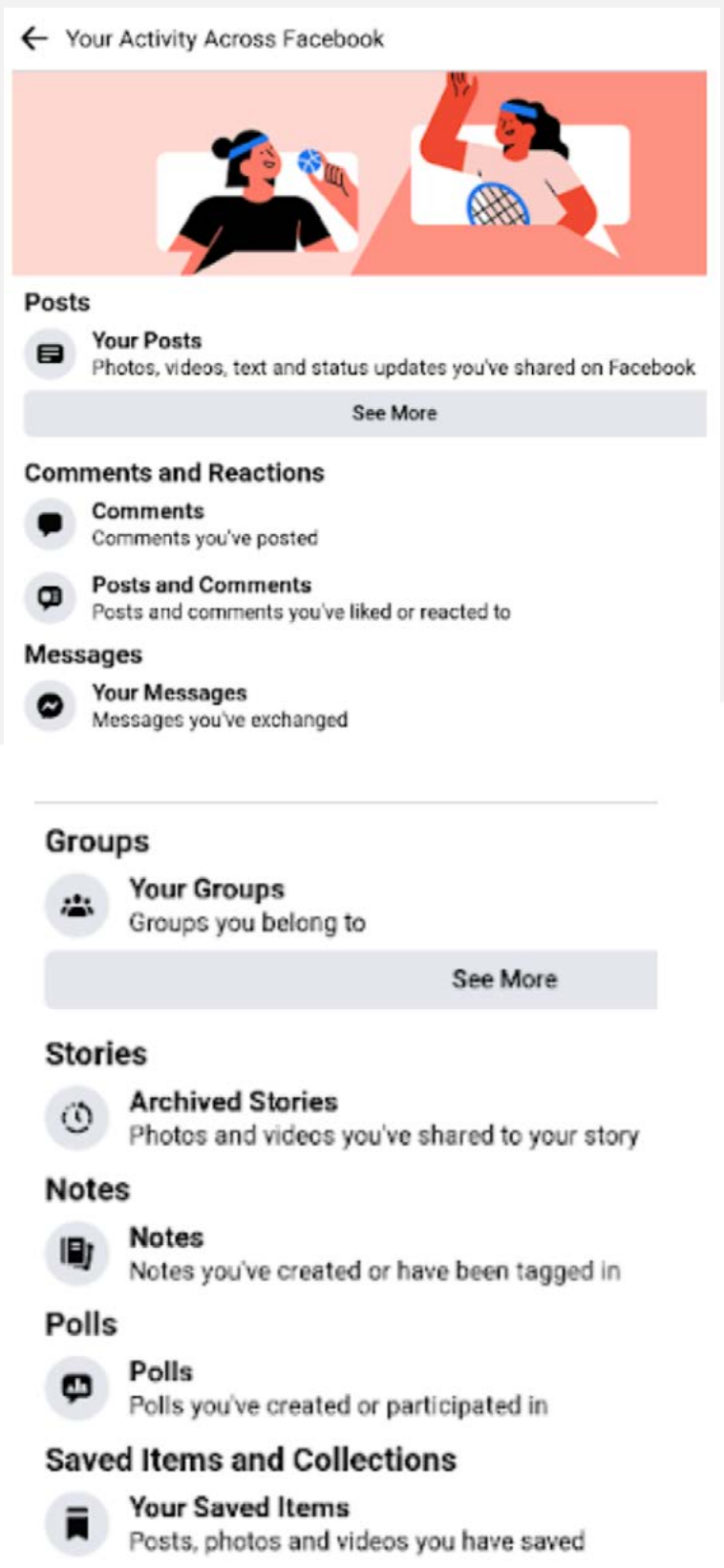


How to access your Facebook information

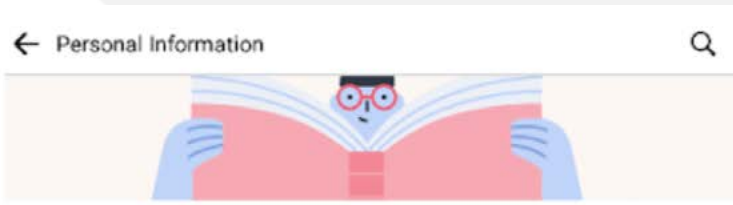
+ Log in to the Facebook account using the **email address and password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and select **settings and privacy**.
+ Now select the **privacy shortcut** option.
+ Select your **Facebook information**.
+ Select **access your information**.

Your activity across Facebook

+ This option allows you to review many of the essential controls relating to posts, photos, videos, comments, messages, groups, and many more. Each setting should be reviewed individually to ensure it's appropriate for your child.



+ Adult Facebook users should also take a moment to familiarise themselves with these settings to protect their own accounts.



Personal Information

Facebook Accounts Center

Accounts Center
Control settings for connected experiences such as logging in and sharing stories and posts across the Facebook app, Instagram and Messenger.

Profile Information

Your Account Creation Date
The date you created your account
23 Jun, 2021

See More

Your Address Books

Your Address Books
Contact information you've added for friends and other people

Your Reward Cards

Your Reward Cards
Reward cards you own

Friends and Followers

Friends
People you are currently connected to

Friend Requests Sent
Requests sent to others to ask them to be friends on Facebook

Friend Requests Received
Requests from others asking you to be friends on Facebook

Removed Friends
People who you are no longer connected with on Facebook

Who You Follow
People, organizations, or businesses that you choose to see content or posts from

People Who Follow You
People who follow you

Logged Information

Search

Your Search History
Words, phrases and names you've searched for

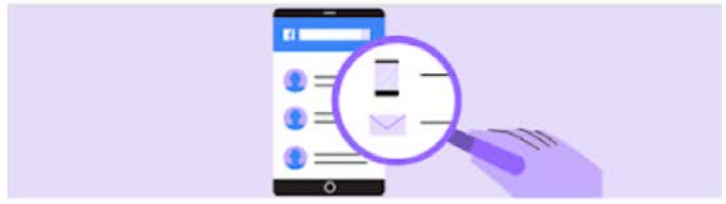
Videos You've Searched For
Videos you've searched for

Voice Search History
A history of your voice search recordings and transcriptions on Facebook

Location

Location History
A history of precise locations received through your devices

Primary Location
Your primary location



Security and Login Information

Where You're Logged In
Periods of time you've been actively logged into Facebook

Authorized Logins
The computers and mobile phones you've saved to your Facebook account

Logins and Logouts
A history of your logins and logouts on Facebook

Apps and Websites off of Facebook

Posts From Apps and Websites
Posts from the apps you've given permission to post on your behalf

Your Apps
Apps you're the admin of

Your Off-Facebook Activity
Your activity from the businesses and organizations you visit off of Facebook

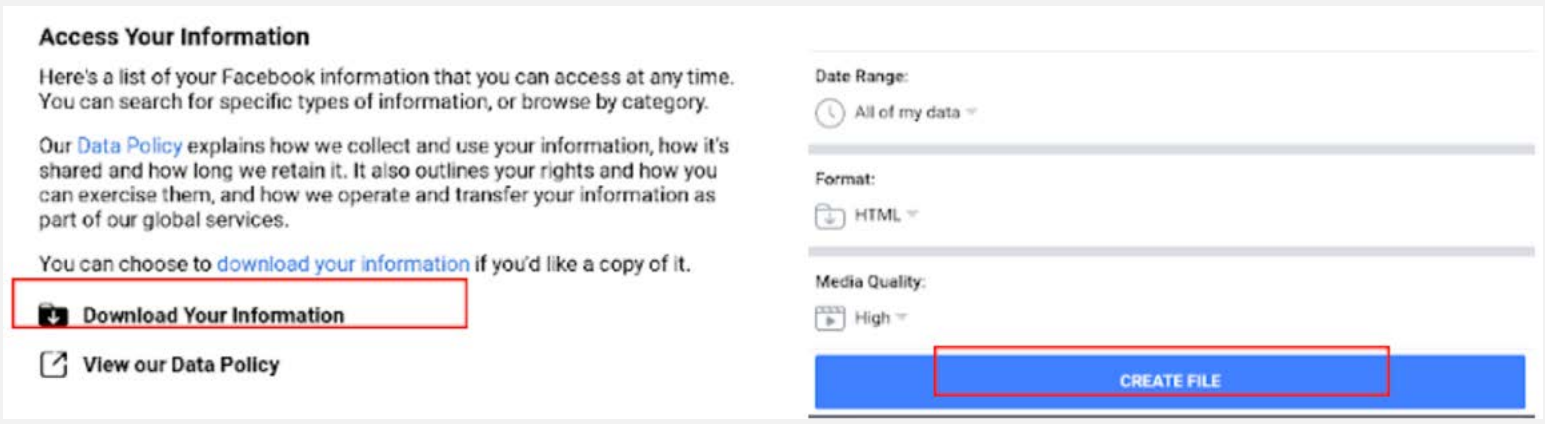
Apps and Websites
Apps and websites you currently have connected to your Facebook

Your News Subscriptions
News accounts that you can use to browse and read news articles on Facebook

Preferences

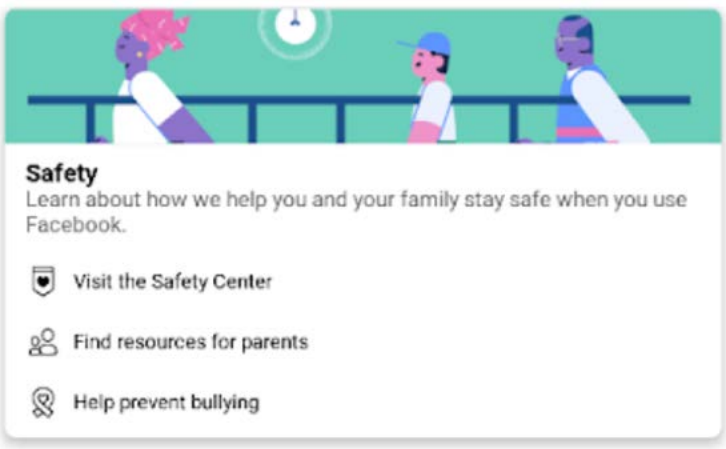
People and Friends

Favorites
Friends and Pages whose posts you've prioritized in your News Feed.



How to access and download all of your Facebook activity and information

+ Log in to the Facebook account using the **email address and password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and select **settings and privacy**.
+ Now select the **privacy shortcut** option.
+ Select your **Facebook information**.
+ Scroll down and select **download your information.**
+ On the screen that opens up, scroll to the bottom of the screen and select a **date range** if you're looking for specific information. Otherwise, select **create file** to download all content.



How to access the Facebook Safety Centre for parents

+ Log in to the Facebook account using the **email address and password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and select **settings and privacy**.
+ Now select the **privacy shortcut** option.
+ Select **find resources for parents.**
+ There is a vide variety of options regarding educational content for parents here:
    + **Get to know Facebook**
    + **Parenting tips**
    + **Expert advice**
    + **Our family of companies**

How to change settings manually

+ Log in to the Facebook account using the **email address and password**.
+ Select the **three lines** in the top-right of the screen.
+ Scroll down to the bottom and select **settings and privacy**.
+ From here you will be able to access all of the above settings. Using **privacy shortcuts** allows you to use these settings far faster.

Other important settings

Many of these settings were covered in the previous instructions, but to make sure you have all the information you need, we'll break down what each section of the settings entails.

General

This section allows you to change the account holder's contact information, where you can direct any notifications to your own email inbox. From here, it's also possible to deactivate the account if you change your mind in the future.

Security and login

You can change the password for the account here. We strongly advise that you activate two-factor authentication with an authentication app, as this allows you to control who logs in and when, keeping your child safe. You can also see what devices are connected to the account. Check here regularly for any devices you don't recognise and deactivate them.

Your Facebook information

This is an important setting as it permits you to view and download all activity history on the account. It's also possible to delete the personal information Facebook has gathered.

Privacy

This setting determines whether the account profile is **public, only friends**, or **customised.** From here, you can manage:

+ Who can see the account activity.
+ Who friend requests can be received from.
+ Who can access personal information connected to the account.
+ Who can make contact with the account holder.
+ Whether the account profile will appear in search engine results.

Timeline and tagging

Another important setting which allows you to adjust whether others can tag the account in photos or posts of their own. This should always be restricted so you can review any posts where the account is tagged.

Blocking

If you feel there's a need to block particular people, you can do it here. It stops them from viewing the account, sending messages, and inviting the account to events. It's also possible to block entire Facebook pages.

Face recognition

When turned on, it allows Facebook to recognise the user in photos or videos. We strongly advise you to disable this feature.

Public posts

From here, you can regulate access to the accounts' public posts, including who can follow, like, or comment.

Controlling the News Feed

It's possible to review and block content on a post by post basis:

+ On any post, select the **three dot icon** in the top-right corner of the post.
+ A drop-down menu will give four options from which you can:
    - » Hide the post from the feed.
    - » Snooze the source for 30 days.
    - » Unfollow the source.
    - » Give feedback on the post.

How to verify the source of the content posted on Facebook pages

+ Select the name of the profile who has posted the post in the newsfeed on a PC.
+ Under the post's cover photo, select the more information icon in the bottom-right corner.
+ Hover the mouse over it to see '**show more information about this link**' and select it.
+ An '**about this website**' popup will appear.
+ Some basic information about the host will become available, such as a brief summary of what the profile host does, how long they've been on Facebook, and when the post was shared.
+ If you don't trust the source, use the tools outlined above to report, unfollow, or block them.

How to review privacy settings using a smartphone

+ Open the **Facebook app** on your device.
+ Select the **settings** option via the three dots under the profile's name.
+ Scroll down to **'view privacy shortcuts'** - there's a picture of a padlock next to it.

Under the **privacy** option, you can review the information and decide who should be able to access it. Review each of these and set them as appropriate to the specific needs of the user.

There are a number of different situations you can customise. For each one, you can choose to share it with the **public, friends,** or **only me**.

+ Email
+ Birthday
+ Relationship
+ Current city
+ Friend and following
+ Future posts
+ Limit past posts
+ Blocking

How to keep your account secure

Here, you can review your password settings and get notifications if your account is accessed from an unknown device or location.

How people can find you on Facebook

This option lets you edit who can send you friend requests and who can look up your name and email address.

Your data settings on Facebook

Review the apps and websites from other companies you've used Facebook to log into and have regularly used. You can remove any that you no longer use here.

By taking your time and slowly going through each of these settings, it's possible to customise the level of privacy in the account. However, while this may prevent unsolicited contact with children, children will still encounter posts and content created by strangers. This is why it's so important to regularly monitor their newsfeed, friends list, likes, shares, comments, and messages.

Messenger Kids

With the rise of social media, and its popularity amongst kids, it's no surprise that there have been platforms created specifically for them. Enter Messenger Kids - an app intended for use specifically for children under 13 years of age. The app works off of the Facebook platform. It does offer good protection for children online in comparison to some of the other more popular apps children use that do not afford the same level of protection from inappropriate contacts or content. A parent will need to have created or have an existing Facebook account for a child to use this app.

Restrictions available:

+ Inappropriate content
+ Contact supervision
+ Chat history review for parents
+ Time restrictions
+ Log out controls

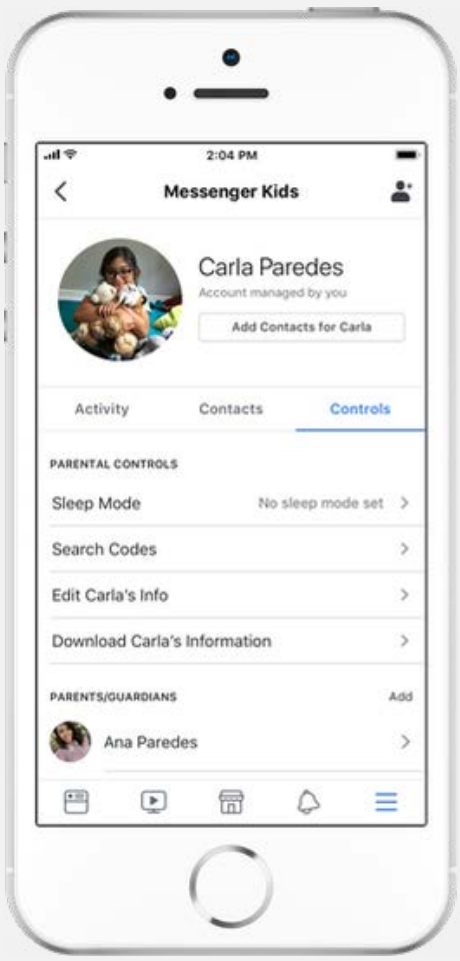
Let's take a more detailed look at how to make your child's Messenger Kids account safer.

How to use set up a Messenger Kids for your child

+ **Install** the app from your preferred app store.
+ On set up, you will need to have your own Facebook account to verify that you are a parent setting up the app.
+ Select **confirm** and enter your own **Facebook login details**.
+ Enter your child's **name** when prompted and select **continue**.
+ On the next screen, select their **date of birth** and then **continue**.

NOTE: We always strongly advise not to use their real personal information.

+ On the **things we want you to know page**, read the information carefully before selecting **OK** to continue and accept the terms and conditions.
+ On the screen that appears next, you will see the names, images, and details of your contacts who have created a Messenger Kids account. Only children of contacts from your own contact list can be approved.
+ You can send and receive invitations to your contacts. When finished, select next.
+ Children will have to be approved by you before they will be able to engage with your child. When finished, select next.
+ You'll then be asked to choose adults who your child can engage with. These may be grandparents, uncles, aunts, or whoever else.
+ Next, you'll be prompted to assign a role of moderator to these contacts for the child's account. We would advise against this.
+ The app will provide a **four-word passcode** which can be used by other children to find your child's account.
+ Next, you'll be asked to approve access to media on the device, to access the camera and microphone, and to receive notifications. Select **agree** to continue.
+ Finally, select **we agree** to verify you have read the terms and conditions.



The parent's dashboard

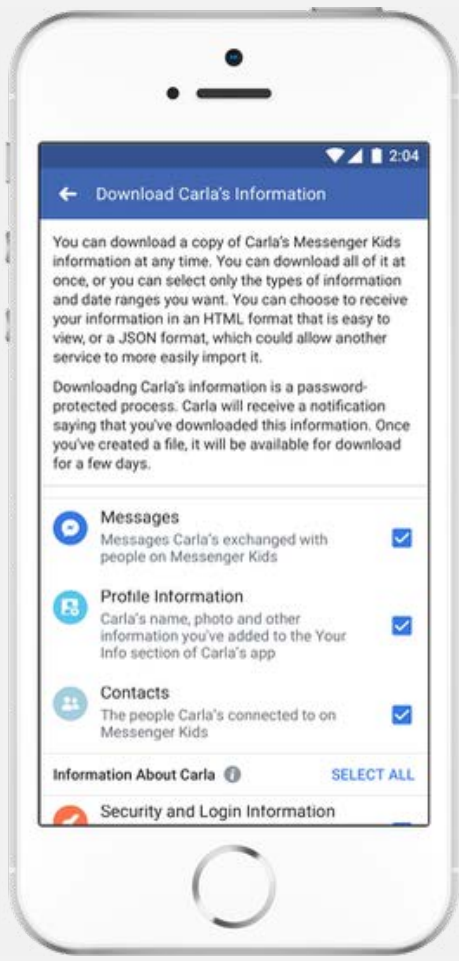
The parent's dashboard is how you can monitor your child's activity on the platform.

How to view recent contacts and chat history
Select **activity** on the left of the screen. Both the recent video and text chat history will be available from the last 30 days.

How to download a child's activity on the platform

+ Open the app.
+ Under **parental controls**, select download [your child's name] information.
+ Select **messages**, **profile information**, and **contacts**.
+ You can choose to download activity or the activity between specific date ranges.
+ Please note that the child should be unable to delete any of their activity.
+ Select **create file** to download.

Log of images in chats
This option allows you to review the child's in- and outbox and see the most recent photos and videos. If there is any content of concern, you can remove or report it.

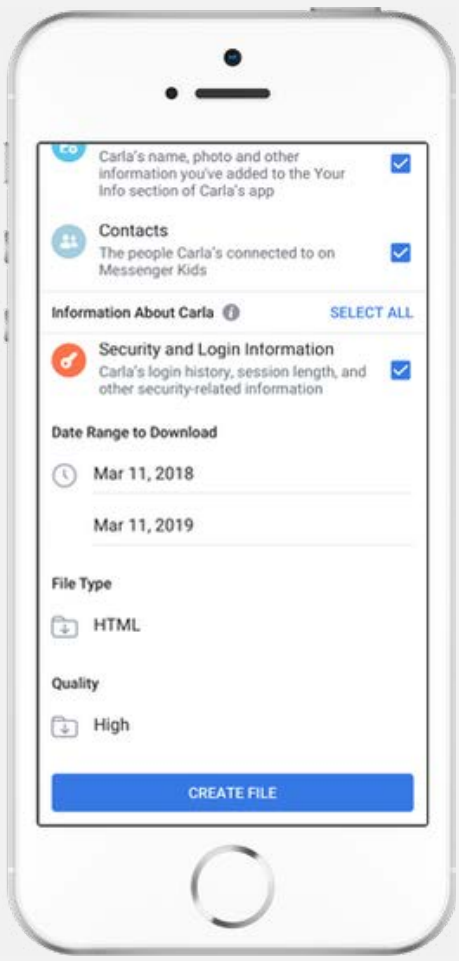


Reported and blocked contacts history

Access a list of the reporting and blocking actions your child has done. You'll see a list of the contacts your child has blocked and/or unblocked, if they have reported any messages, and any contacts they've reported and the reason for their action. Parents will continue to be notified via Messenger if their child blocks or reports someone.

Remote device logout
It's possible to see all devices where your child's account is logged in to Messenger Kids. If there are any devices you don't recognise, you should immediately log the device out of the app.

Compared to other social media platforms, a lot of effort has gone into this one to make it as child-friendly and safe as possible. With that in mind, you should still take the time to look through all the settings, checking in frequently, to ensure your child stays protected.



Houseparty

Houseparty is a social network that's main focus is on face-to-face interaction. It's seen a huge increase in users primarily because it's very simple to use and easy to host group video chat. You can also play games on the platform - a key feature that became very appealing to many during lockdown. The app has been around since 2016, but after being bought by Epic Games, the company behind Fortnite, in 2019, its popularity skyrocketed. Users can now connect to other Fortnite players through an in-built feature. Since Fortnite is incredibly popular with kids, it stands to reason Houseparty would be too.

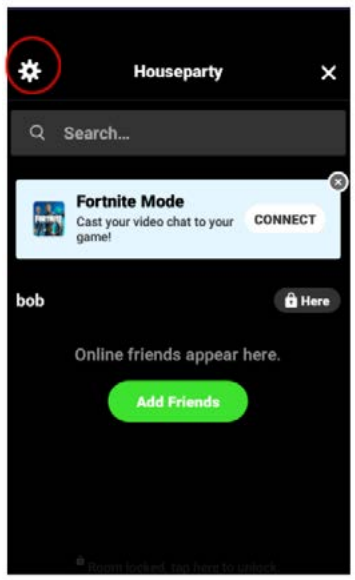
Restrictions available:

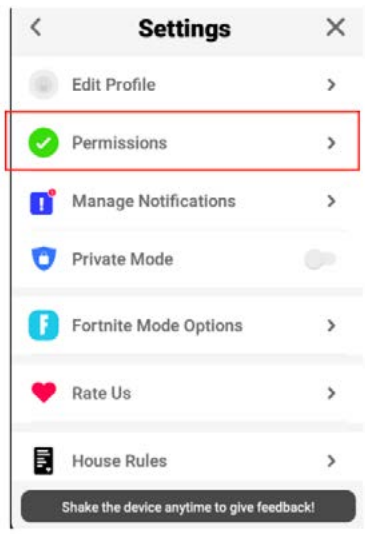
+ Online chat restrictions
+ Online privacy
+ Restrict access
+ Restrict data sharing
+ Sharing location

Let's take a look at how to navigate this app.

How to lock a room

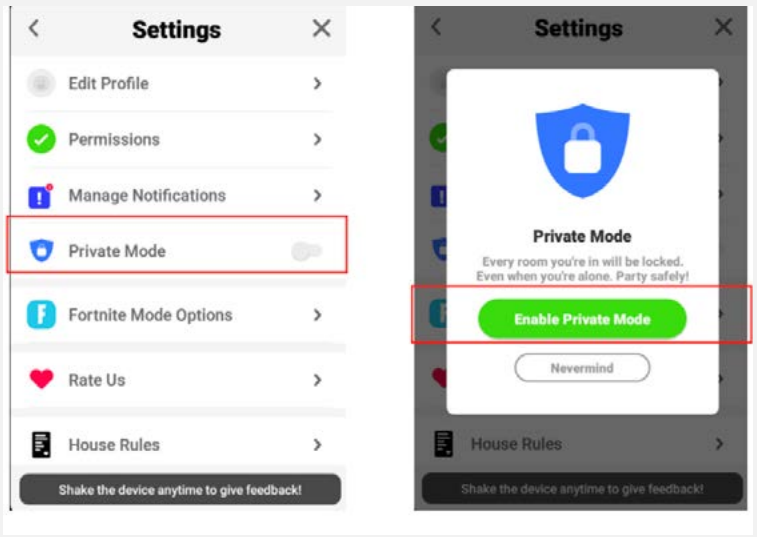
+ Open the **Houseparty app**.
+ Select the **lock icon** in the middle of the bottom of the screen.
+ Once activated, only invited participants will be able to access the room.
+ To unlock the room, simply select the **lock icon** again.





How to secure the user's location setting

+ Open the **Houseparty app.**
+ In the top-left corner of the screen, select the **face icon** which opens the friends menu.
+ From the screen that opens up select, the **cog icon** at the top-left corner to open settings.
+ Then select the **permissions** option.
+ At the bottom of the permissions menu is the option to **enable location** or **disable location**. If left **enabled**, others will be able to make contact based on the location of the device. We recommend switching it to **disabled**.

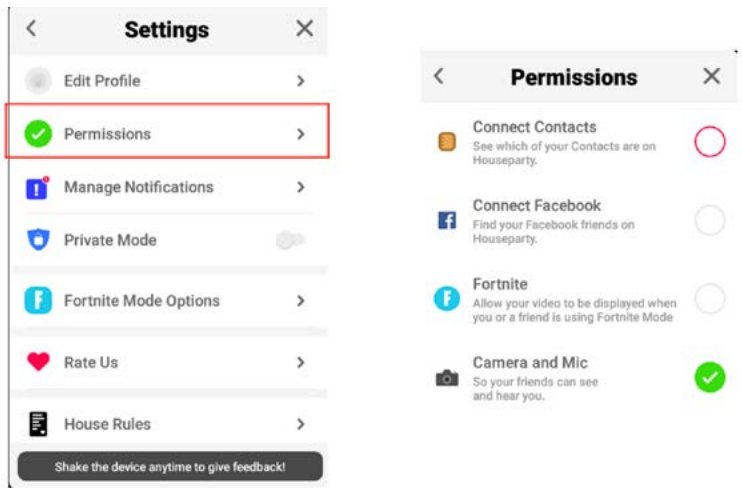


How to enable Private Mode

+ Open the **Houseparty app.**
+ In the top-left corner of the screen, select the **face icon** which opens the friends menu.
+ From the screen that opens up select, the **cog icon** at the top-left corner to open settings.
+ Select **Private Mode**.
+ Select **'enable Private Mode'.** Under **Private Mode**, every room the user goes into will be locked by default.

Managing friend notifications, reporting, and blocking others

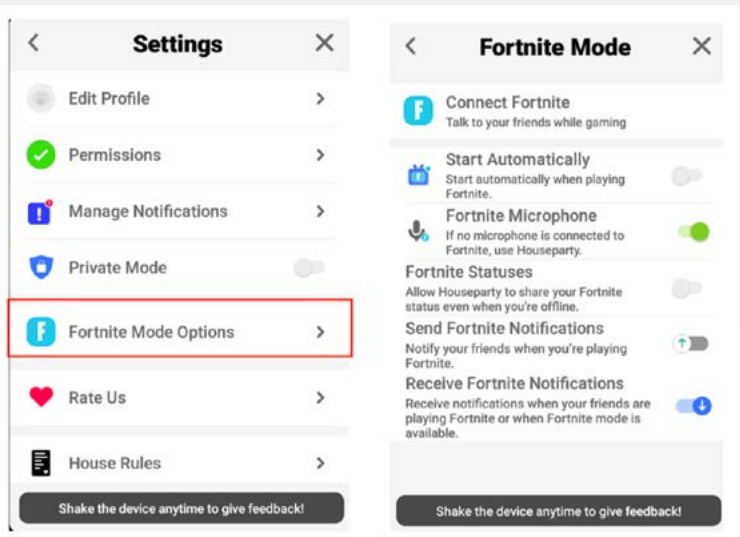
+ Open the **Houseparty app.**
+ In the top-left corner of the screen, select the **face icon** which opens the friends menu.
+ A list of friends will appear. Choose the profile you wish to manage and select the **three dots**.
+ Four options now become available:
    + **Ghosting**
    + **In the House**
    + **Unfriend**
    + **Report or block**
+ To block or report an inappropriate person, choose the appropriate option.



How to disconnect social media apps linked to Houseparty

Houseparty encourages users to connect to their contacts from other social media platforms. This should be restricted to prevent unwanted contacts.

+ Open the **Houseparty app.**
+ In the top-left corner of the screen, select the **face icon** which opens the friends menu.
+ From the screen that opens up select, the **cog icon** at the top-left corner to open settings.
+ Then select the **permissions** option.
+ On the screen that opens up, toggle as required.
+ To disable the feature, deselect the appropriate option, e.g. **'connect Facebook'.**



How to connect to a Fortnite account

This feature can result in unwanted direct contact with children and teens. It's essential for parents to be aware of this feature and what connections and notifications are available.

+ Open the **Houseparty app.**
+ In the top-left corner of the screen, select the **face icon** which opens the friends menu.
+ From the screen that opens up select, the **cog icon** at the top-left corner to open settings.
+ Select **Fortnite Mode** options.
+ On the screen that opens, there are several options:
    - » Connect Fortnite -Connects to the Epic Games Fortnite account
    - » Start Automatically - Activates the Houseparty app and connects with connected friends once the game opens
+ Other options can be seen in the image above.

Instagram

You will no doubt have heard of Instagram. It's currently the second biggest social media platform, with 1.2 billion monthly users. And its connection to Facebook only makes it that much bigger. So it will probably come as no surprise that your child wants to take part. But there's much to be done if you want to keep them as safe as possible.

Restrictions available:
+ Inappropriate content
+ Social networking
+ Cyberbullying
+ Privacy and identity theft
+ Chatting

What options are available on Instagram?

How to set an Instagram account to private
+ Open the **app**.
+ At the bottom right-hand corner of the screen, select the **profile icon**.
+ Select the **three horizontal lines** icon in the top-right corner of the screen.
+ Next, choose the **settings option** at the very bottom right of the screen.
+ Go to privacy and then **account privacy.**
+ Activate a **private account** by setting the button to on.

How to block comments
+ Open the **app**.
+ At the bottom right-hand corner of the screen, select the **profile icon**.
+ Select the **three horizontal lines** icon in the top-right corner of the screen.
+ Next, choose the **settings option** at the very bottom right of the screen.
+ Select **privacy** and then **comments**.
+ In the **controls** section, set the **'allow comments from'** to whichever you prefer, likely **'people you follow'**.
+ Under the same heading, there's also an option to 'block comments from'. By activating this feature, any new comments from people you block won't be visible to anyone but them.

How to hide offensive comments
+ Open the **app**.
+ At the bottom right-hand corner of the screen, select the **profile icon**.
+ Select the **three horizontal lines** icon in the top-right corner of the screen.
+ Next, choose the **settings option** at the very bottom right of the screen.
+ Select **privacy** and then select **comments**.
+ Under **filters**, activate the option by pressing **'hide offensive comments'**.
+ You can also use the **manual filter** to enter specific words or phrases you wish to block.

Control who can tag you in a post

+ Open the **app**.
+ At the bottom right-hand corner of the screen, select the **profile icon**.
+ Select the **three horizontal lines** icon in the top-right corner of the screen.
+ Press the **settings option** at the very bottom right of the screen.
+ Select **privacy**, then **tags**.
+ Next, choose **manually approve tags**. Any post tagging this account will now have to be approved.

Restrict comments on Instagram Stories

+ Open the **app**.
+ At the bottom right-hand corner of the screen, select the **profile icon**.
+ Select the **three horizontal lines** icon in the top-right corner of the screen.
+ Choose the **settings option** at the very bottom right of the screen.
+ Select the **Story** option.
+ Under the allow message replies heading, there are three options. Choose the one you are most comfortable with, probably either 'people you follow' or turn them off altogether.

Restrict sharing of Instagram Stories

+ Open the **app**.
+ At the bottom right-hand corner of the screen, select the **profile icon**.
+ Select the **three horizontal lines** icon in the top-right corner of the screen.
+ Choose the **settings option** at the very bottom right of the screen.
+ Select the **Story** option.
+ Under the heading 'sharing' there are three options which can be activated or deactivated as required. You'll likely want to turn all of them off:
    + **Allow resharing to Stories** – Anyone can add your feed and IGTV videos to their stories. Your username will always show up with your post.
    + **Allow sharing** - Let others share photos and videos from your stories as messages.
    + **Share your Story to Facebook** – Automatically share photos and videos from your story to your Facebook story.

How to remove unwanted followers

+ Open the **app**.
+ Search for the profile by selecting the magnifying glass at the bottom-left of the screen.
+ Select the **profile** to open it.
+ Press the **three dots** in the upper right corner of the profile screen.
+ Then select **block** and/or **report**.

Instagram is one of the most popular social media platforms, so if your child wants a social account, it will likely be for this one. When it comes to sharing pictures, you have to be extremely careful. Make sure your child knows what they should and shouldn't share, and regularly check to see who is following and messaging them.

Snapchat

Snapchat - or 'Snap' as your child might call it - is another image-based sharing app. The platform is popular amongst adults, teens, and younger kids alike, making the choice to allow your child to use it a difficult one. While having a parental guidance rating in only some countries, this app isn't suitable for children under 13 years of age.

Restrictions available:

+ Inappropriate content
+ Sharing location
+ Block/ignore
+ Privacy

Unlike some of the other apps we've mentioned so far, Snapchat has a lot of unique terms that are worth familiarising yourself with. So before we dive into the various settings, let's look at some of the expressions you'll likely want to know.

Snapcode
This is similar to a QR code which other users can scan with their phone to identify and connect quickly to another account.

Geofilter
This is the app's ability to recognise where you are physically in the world at the time of use. The information can be shared with others in the content you create or to notify others where you are on the Snap Map. This setting should be disabled on children's accounts (more on that later).

Snap Map
This feature allows you to share their location in real time with other Snapchat users. It can be set to three settings: public, ghost mode, and off. The feature can also be used to locate other Snapchat users. This setting should be disabled on children's accounts (more on that later).

Snap
A generic term for a photo or video which has been taken, posted, or shared with other Snapchat users.

Story
The Snapchat Story feature allows you to combine several snaps that have been taken and then present it as a Story which is shared publicly. The Story can be saved as a Memory, and if not, they disappear after 24 hours.

Snapstreak
This relates to Snapchat users who have shared content with each other every day. The higher the Snapstreak, the longer the time content has been shared on a daily basis with another user.

If you spend enough time around Snapchat, you'll hear these terms regularly. Hopefully this small glossary will help you understand what your child means and what they hope to do with the app.

How to enable two-factor authentication
+ Open the **app**.
+ In the top-left corner of the screen, select the **person icon**.
+ Select the **cog icon** in the top-right corner of the screen.
+ Select **two-factor authentication**.
+ Select **continue**.
+ Two options will be available: text verification and authentication app. We strongly advise in favour of using an authentication app.
+ Follow the onscreen prompts.

How to review the friends list
+ Open the **app**.
+ In the top-left corner of the screen, select the **person icon**.

+ Scroll down friends and select my friends.
+ You can also access the contacts list by selecting the speech bubble at the bottom of the screen.
+ A full list of the current contacts will appear. These should be reviewed regularly by parents, with strangers removed.

How to review the notification settings

+ Open the **app**.
+ In the top-left corner of the screen, select the **person icon**.
+ Select the **cog icon** in the top-right corner of the screen.
+ Select **notifications**.
+ There are a large number of permissions the app wants access to. Please review each individually. Notifications can be distracting and they often encourage overuse. The specific options available are:
    - » **Enable notifications**
    - » **Stories from friends**
    - » **Friend suggestions**
    - » **Mentions**
    - » **Memories**
    - » **Friends' birthdays**
    - » **Message reminders**
    - » **Creative effects**
    - » **Best friend message sounds**
    - » **Wake screen**
    - » **Blink LED**
    - » **Vibrate**
    - » **Sound**
    - » **Ring**

How to review the notification settings for Stories or subscriptions

+ Open the **app**.
+ In the top-left corner of the screen, select the **person icon**.
+ Select the **cog icon** in the top-right corner of the screen.
+ Select **notifications**.
+ At the bottom of the notifications list under **Stories that I follow,** select manage **Story notifications**.
+ In the **Story notifications** page that opens up, you should regularly review the friends and subscriptions to ensure they're age appropriate for your child.
+ To unsubscribe, simply **untick the box** relating to the subscribed account.

How to review the privacy and location settings

+ Open the **app**.
+ In the top-left corner of the screen, select the **person icon**.
+ Select the **cog icon** in the top-right corner of the screen.
+ Select **contact me** and choose either **everyone** or **my friends**.
+ Return to the previous menu and then select **who can view my story** and choose either **everyone, friends only,** or **custom**.
+ Go back to the previous menu again and select see me in quick add. This allows users to make contact with mutual friends or other connections. For younger children, it's recommended you **deselect this option**, which is activated by default.
+ Again, return to the previous menu and select **my location**.
+ Ensure **ghost mode** is enabled for young users to prevent sharing location information.
+ There's an option under **who can see my location** to share the user's location. There are a few options available, but we strongly recommend against it.
+ There is also an option for **location requests** to **allow friends to request my location**; this is enabled by default and should be **disabled**.

How to disable ads

+ Open the **app**.
+ In the top-left corner of the screen, select the **person icon**.
+ Select the **cog icon** in the top-right corner of the screen.
+ Scroll down to **features**.
+ Select the **ads** option.
+ Select **advert preferences**.
+ Deselect the following targeted advertising options which are **activated by default**:
    - » **Audience-based**
    - » **Activity-based**
    - » **Third-party ad networks**

This should give you a good idea of what needs to be done to keep your children safe. Snapchat is all about content that disappears when viewed, so it will be impossible for you to see what your child has been viewing. The more you can lock down their privacy settings, the safer they'll be.

TikTok

TikTok is, essentially, a video sharing app with a music-themed twist. It allows users to create, share and watch content posted by others on the app. One major feature of TikTok is being able to 'duet' with others, adding your video to theirs. Due to this level of interactivity between users, we would recommend parental guidance for its use. Even though it's extremely popular with teenagers, it also has a burgeoning adult audience, so a rule of thumb is to keep your eye open for any mature content unsuitable for children under 13. Personally, we believe TikTok shouldn't be available to any under 15 if at all.

What we will say in the company's favour is that it has been actively improving its safety advice content and portal since 2021.

Restrictions available:
+ Online chat restrictions
+ Online privacy and identity theft
+ Restrict access
+ Restrict content
+ Restrict data sharing
+ Sharing location

Before we begin, we have some immediate concerns relating to the use of this app by children and strongly advise against it.

When creating a TikTok account, users are asked to sign in using an existing social media account. If they sign up this way, the app has access to the user's contacts and other information on that platform. It's also well-known that TikTok collects a multitude of personal information from its users. This relates to technical and behavioural information, location, shared social network information, messages, metadata, contacts, and more.

There is also a considerable amount of inappropriate content on this platform that's entirely unsuitable for children. Some of this even appears under the 'recommended for you' feature of the app regardless of the setting. A graphic beheading video managed to make it onto the platform in June 2021 after it was placed in the middle of a harmless looking piece of content. This type of content can also bleed onto social media platforms, so parents are always advised to preview any content young children are going to view. It can be easy to find inappropriate content due to the ability to add #hashtags.

The app, which was originally known as Musical.ly, was primarily a platform that encouraged users to mime songs. Even then, there was a risk that some of the songs may have contained sexually graphic or explicit lyrics. The app has evolved far beyond this and you could literally find anything on it. It has been responsible for a far higher number of online challenges than other social media platforms. Many of these are harmless, but others, not so.

TikTok also has a feature where users can make in-app purchases of gifts or coins they can share. This is designed to encourage creativity among the community. Virtual coins can be exchanged for real world money if the user gets enough, with 10,000 coins being worth roughly €100. The monetisation of content encourages users to come up with more creative or extreme content. You can toggle off "in-app purchases" in the restrictions section.

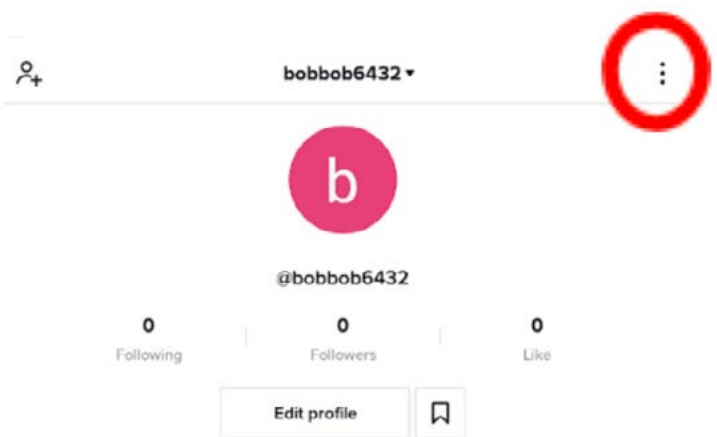
The parental controls for TikTok specifically refer to "your teen". Parents should take strong notice of this message. This platform is not in any way intended for young children and they should

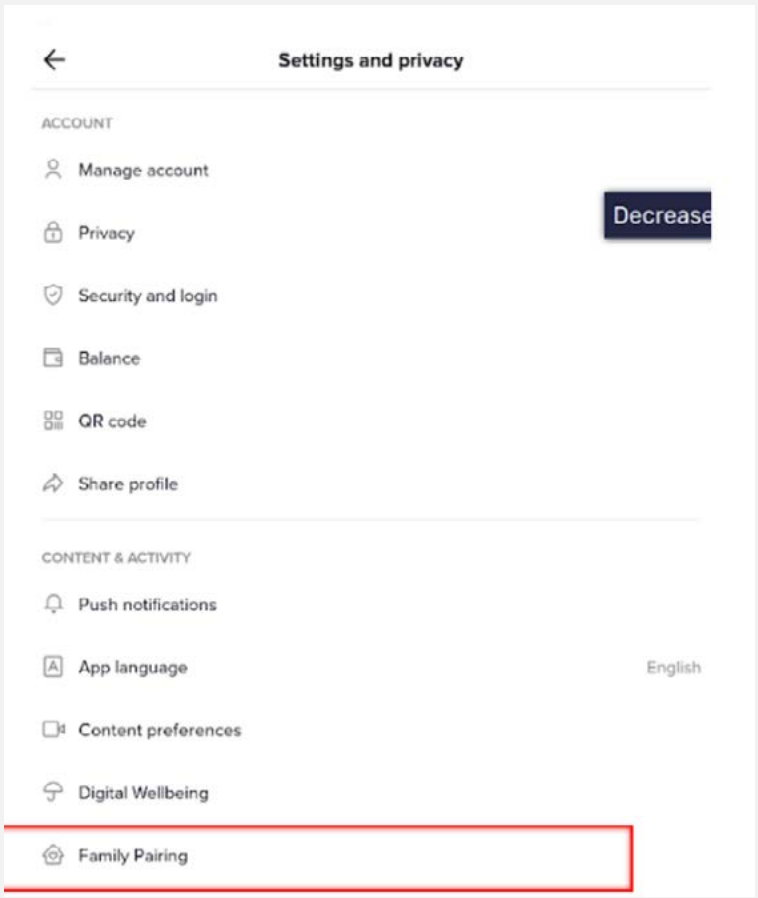
never be afforded access to it.

A negative that we often observe when setting up parental controls is the requirement to access your teen's device. This is an issue which can cause some heated arguments in the home. Often, teens don't want to give away access to their digital devices, especially to their parents. Our stance on this is very clear: without parental access, monitoring, and supervision, no teen under 15 should have access to a digital device.

Setting up a TikTok account

+ **Download TikTok** from the Google Play Store or Apple App Store.
+ Open the **app**.
+ Sign up for TikTok by selecting the most relevant option:
  - » Use phone or email
  - » Continue with Facebook
  - » Continue with Google
  - » Continue with Twitter
+ Next, you'll be prompted to enter a **date of birth.** We strongly advise that you never enter the correct date of birth, the reason being that, in the event of a data breach, your personal information won't be accurate.
+ On the next screen, you can select specific themes or content you might prefer. If you're not planning on using this yourself, you don't have to bother.
+ You should be taken to the **TikTok home screen.**
+ For future reference for the rest of the instructions, you will need to go to your profile page to access the settings. To get here, select the **person icon** in the bottom-right corner of the screen. It should have your chosen name under it.
+ Then select the **three dots** in the top-right corner to access the settings.



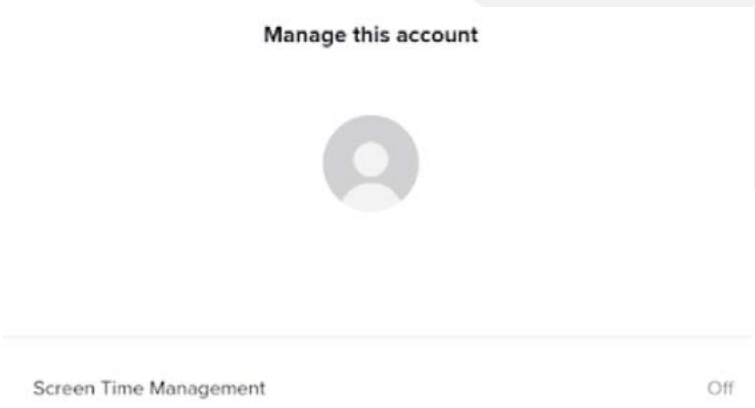


Using the family pairing option

+ In the settings, scroll down to the **content & activity** section and select **family pairing**.
+ Here you have the ability to:
  - » Set a limit on your teen's watch time.
  - » Limit content that isn't suitable for your teen.
  - » Manage your teen's privacy and safety settings.
  - » Choose whether your teen can have a private or public account.
+ Select **continue.**
+ On the next Family Pairing screen, you are prompted to enter if the account is for the parent or teen. **Select parent.**
+ You'll see a QR code. On your teen's device, open up TikTok, navigate your way to the family pairing option, but this time **select teen.**
+ **Scan the QR code** with your teen's device to link them.
+ Once the QR code has been scanned, select **'link accounts'** at the bottom of the screen.

Let's run through some of the options available to you as a parent account...

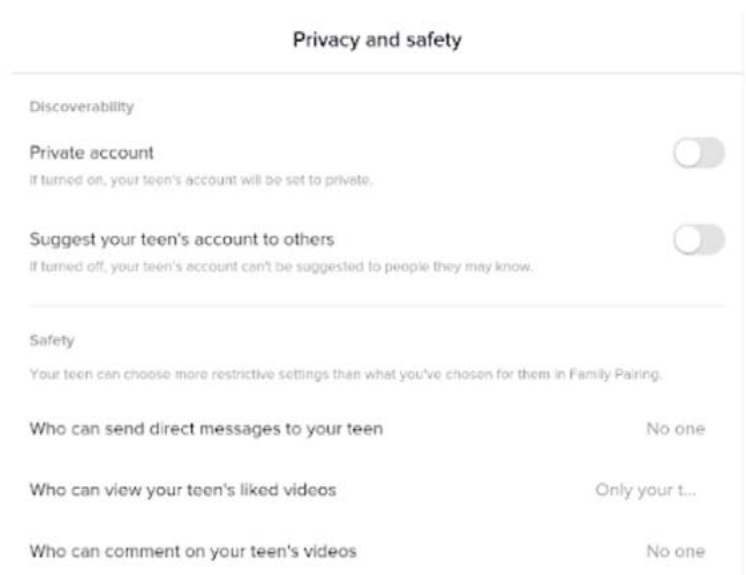
Screen time management
Here, you can set a limit on how long your teen is able to use TikTok. Once they reach the limit, they won't be able to use the app anymore unless you use a passcode to unlock it. If screen time management is on, your teen won't be able to log out or switch to another account.



Set a time limit
The default setting is for one hour. Unfortunately, the lowest limit a parent can set is 40 minutes. The options are:
+ 40 minutes
+ 60 minutes
+ 90 minutes
+ 120 minutes

Restricted mode
This mode limits content that may not be appropriate for some viewers. If restricted mode is on, your teen won't be able to log out or switch to another account.

To enable, select restricted mode from the menu. At the bottom of the screen, select **restricted mode** to activate.

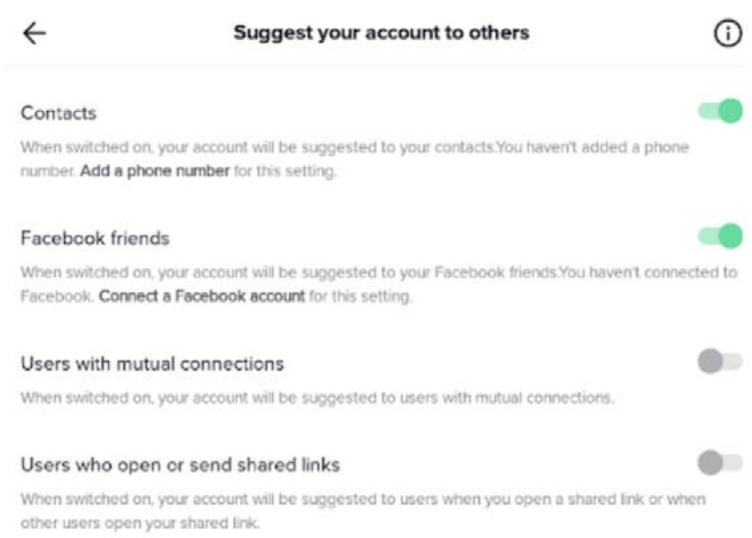


Privacy and safety
Under this option, there are two sections:

Discoverability
+ Private account - If turned on, your teen's account will be set to private.
+ Suggest your teen's account to others - If turned off, your teen's account can't be suggested to people who they may know.

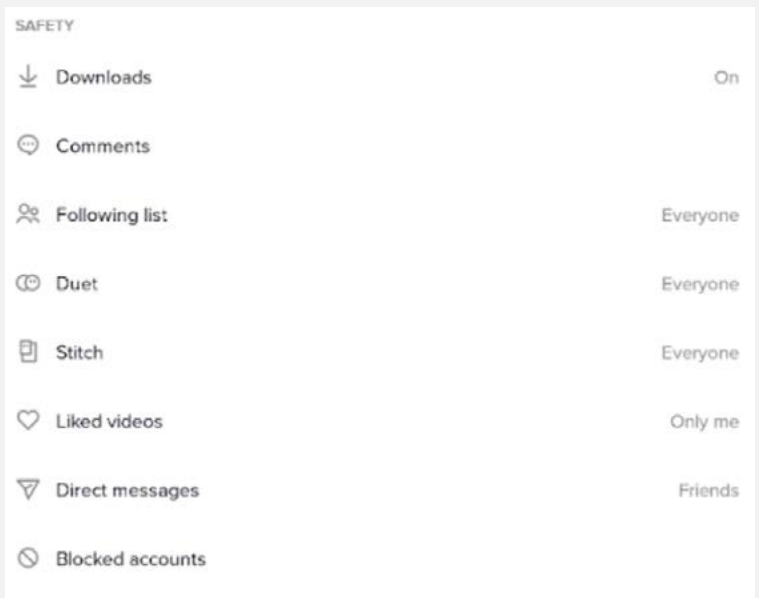
Safety
Your teen can choose more restrictive settings than what you have chosen for them in family pairing:
+ Who can send direct messages to your teen - The options available are everyone, friends, followers that you follow back, or no one.
+ Who can view your teen's liked videos - The options available are everyone, only your teen.
+ Who can comment on your teen's videos - The options available are everyone, friends, followers that follow you back, or no one.

How to set a TikTok account to private and prevent others from finding it
+ From settings, go to the **privacy** section.
+ Activate **private account** by switching the **button to on**. This ensures that only users you approve can follow the account.
+ Directly underneath is the option to **suggest your account to others**.
+ There are several options here to review and set up. Toggle the appropriate settings as required.



Other options available under privacy and settings/safety
There are a number of options to restrict who can interact with the account user

+ From settings, go to the **privacy** section.
+ Under the **safety** option, there are several items which need to be enabled or disabled depending on a child's requirements. Take a look through and change as appropriate.



How to turn on Restricted Mode

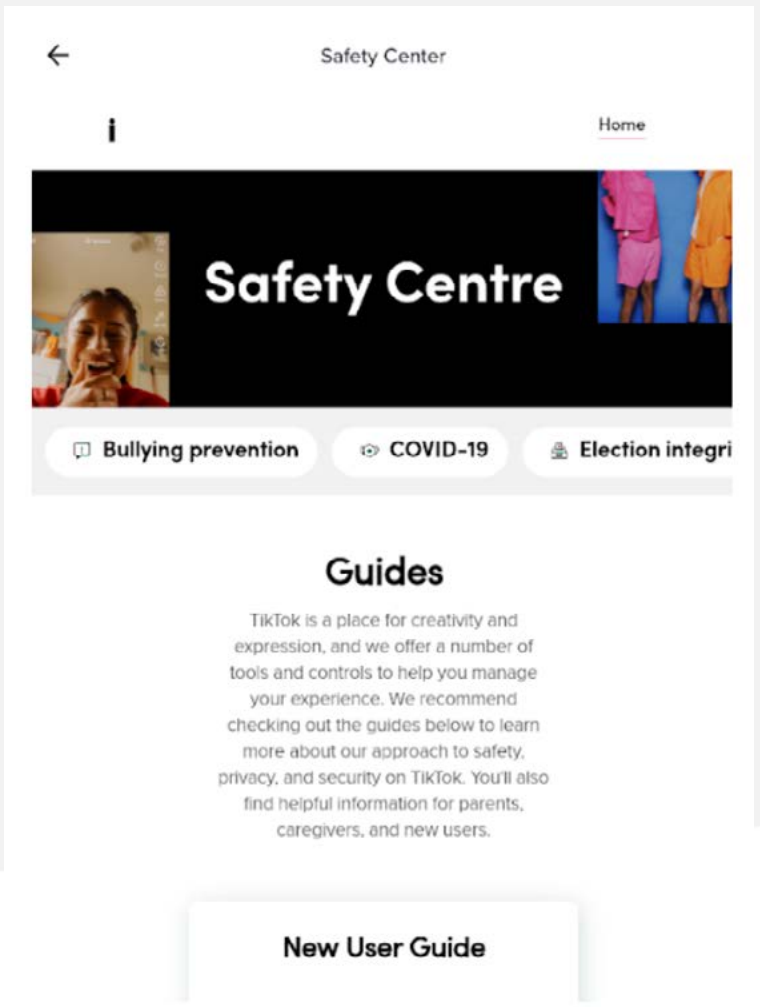
+ From settings, go to the **digital wellbeing** section.
+ Activate **Restricted Mode** by switching the **button to on**.
+ You'll be asked to set a passcode; enter a **4-digit PIN** and press **next**.
+ To confirm the **PIN**, press **next**.
+ The passcode will now be required before restrictive content can be accessed.

How to set up screen time management

+ From settings, go to the **digital wellbeing** section.
+ Select the **screen time management** option.
+ Select **turn on screen time management.**
+ When prompted, set a **4-digit PIN** and select **next**.
+ Confirm the **PIN** and select **next.**
+ The time is now restricted to **60 minutes** per day. To use the app after this time will require the **PIN.**

How to block or report a user

+ If you encounter inappropriate content on the platform, you can report or block the user by first selecting the **user's profile name.**
+ Then on the profile screen, select the **three dots** in the top-right corner of the screen.
+ Select **block** to block the user or **report** to report the user.



How to access the TikTok Safety Centre

+ From settings, go to the **support** section and select **Safety Centre.**
+ Here you will find a huge amount of content under the following headings:
  - » New user guide
  - » Parents and caregivers
  - » Our approach to safety
  - » Privacy and security on TikTok
  - » Safety and privacy controls
+ Read everything you feel you need to know.

WhatsApp

WhatsApp is a very popular messaging, call, and image-sharing app. The many features of this app over time have transformed messaging platforms to become a form of social media in and of themselves. You might even use this one yourself - outside of a phone's regular messaging app, this one is the most popular alternative. It's easy to set up different group chats for various purposes. Thankfully, there are a number of features which will allow you to closely monitor your child's activity. However, they are not at a level that could enable 100% protection or anywhere near it.

Restrictions available:

+ Block accounts
+ Privacy
+ Sharing location
+ Reporting issues

Unlike other apps we've featured so far, this one has a limited number of options available to you.

How to block an account

+ Open the app.
+ In the top-right corner, select the **settings** option.
+ Then select **account**.
+ Next, the **privacy** option.
+ Select **blocked**.
+ You can now add the account you wish to block. A blocked contact will no longer be able to call or send messages.

How to disable personal information

+ Open the app.
+ In the top-right corner, select **settings.**
+ Then select **account.**
+ Next, the **privacy** option.
+ The following four items can now be set to **everyone, my contacts,** or **no one.**
    - » **Last seen** - When the account holder last used the app.
    - » **Profile photo** - The account holder's profile photo.
    - » **About** - The account holder's bio.
    - » **Status** - The account holder's current status.

How to turn off live location

+ Open the app.
+ In the top-right corner, select **settings.**
+ Then select **account.**
+ Next, the **privacy** option.
+ Select **live location** and set it to **none.**

How to report safety and security issues

+ In the top-right corner, select **settings.**
+ Then select **help.**
+ Finally, select **contact us** to forward a message regarding a safety or security issue.

How to monitor content of a WhatsApp account with WhatsApp Web

+ Using an internet browser, go to https://web.whatsapp.com/
+ On the screen, you will see a QR code and the following instructions.
+ Open WhatsApp on your phone and select **settings**.
+ Then select the **WhatsApp Web** option.
+ Then point the phone at the screen to capture the **QR code**.
+ Once the **QR code** is captured, the account and all messages and content will appear on the screen.
+ The account can now be monitored in real-time.

The likelihood is your child will want to use WhatsApp to stay in touch with friends and maybe even family. Because you only tend to talk to people you know through the app, the chances of your child getting in contact with someone unfamiliar to you is unlikely. But through group chats, it isn't impossible, so it's still worth checking in periodically.

YouTube

YouTube is the most popular video-sharing platform. The chances are that you've even used it in the past. Music videos, film trailers, and TV highlights are uploaded frequently, going beyond the platform's original intention of sharing home videos. Today, **500 hours worth of content is uploaded per minute**. That leaves a lot of room for creative content, but also highly inappropriate content. The platform does have some parental controls, however, due to the level of inappropriate content available, its use is not advised for younger children.

To access the parental controls, you'll need a Google account as they now own the platform. But if the child simply signs out of the account or accesses the site through an internet browser that hasn't been logged in, they can work around your restrictions.

Restrictions available:
+ Time limits
+ Inappropriate content

Assuming your child does stay logged in, what can you do to keep them safe?

How to set up restricted mode using a PC
+ On your internet browser, open up https://www.youtube.com
+ If you don't have a **Gmail account**, you'll need to create one.
+ On YouTube, select your **account profile** in the top-right of the screen.
+ From the drop-down menu, select **restricted mode.**
+ Set the toggle to **on** to activate it.

How to set up restricted mode using an Android device
+ Open the **YouTube app.**
+ If you don't have a **Gmail account,** you'll need to create one.
+ **Sign in** to your **Gmail account.**
+ Select your **profile icon** in the top-right corner to access the **settings menu.**
+ Then scroll to **settings.**
+ Now select **general.**
+ At the bottom of the menu is the **restricted mode** option - select to activate.

How to set up restricted mode using an iOS device
+ Open the **YouTube app.**
+ If you don't have a **Gmail account**, you'll need to create one.
+ **Sign in** to your **Gmail account** on the YouTube app.
+ Select your **profile icon** in the top-right corner to access the **settings menu.**
+ Then scroll to **settings.**
+ Now select **general.**
+ At the bottom of the menu is the **restricted mode** option - select to activate.

How to set time limits
While this is a welcome addition to the controls, it only reminds the user to take a break. To activate this feature:
+ Follow the steps above to get to the settings menu on your particular device.
+ Here, scroll to and select **'remind me to take a break'** to activate the feature.

YouTube automatically shows the next video similar to the previous one. This feature is designed to increase engagement and keep users on the platform. Time can soon fly by as users are being fed more and more similar content. This can also lead to more explicit content being seen without the correct filters being applied. We recommend using external software or an app to manage total daily screen time.

YouTube Kids

If you've decided to let your child use YouTube, we strongly recommend you only let them use YouTube Kids, especially those under twelve-years-old. The content on this alternative version of the platform is specifically child-orientated. Even with the best filters in the world, inappropriate content may still be accessed on YouTube. While it may also occur from time to time on YouTube Kids, it happens far less often. If possible, you should still try to view the content young children are viewing first. Always review the content that has been viewed to ensure your child has not been exposed to material which may be distressing to them. It's also possible to set up one account and add several children, each with different parental control settings.

Restrictions available:

+ Inappropriate content
+ Time limits

Despite being designed for kids, there are still some settings we recommend you change.

Setting up a parental control account

+ Open the **app.**
+ Select the **profile image** in the upper left-hand corner of the screen.
+ A dialog box will open which will prompt you to **create a profile**.
+ Select **get started.**
+ Enter the details as required, such as the **year of birth**.
+ You'll be asked to nominate a Google account to connect to your profile.
+ If your account doesn't have **recorded consent**, you'll see a parental consent form.
+ These are terms and conditions which you should read.
+ Once finished, select **done** if you wish to proceed.
+ When prompted, enter your **password.** If your account already has a recorded consent, enter your **password** to confirm your identity.
+ You'll now be prompted to **create a profile** for each child by entering the child's **name, age,** and **month of birth.**
+ ***NOTE: We advise that you don't give accurate details, only approximate, even though only you and your child will have access to this personal information.***

Setting the parental control options

+ To select the appropriate content experience for a child, there are four content settings to choose from:

    » The **preschool** setting is designed for children ages 4 and under. The content available is chosen to promote creativity, playfulness, learning, and exploration. While their system does what it can to remove videos not suitable for kids in preschool, not every video is reviewed manually. If you come across something you think is inappropriate for such a young age, you can block or report it.

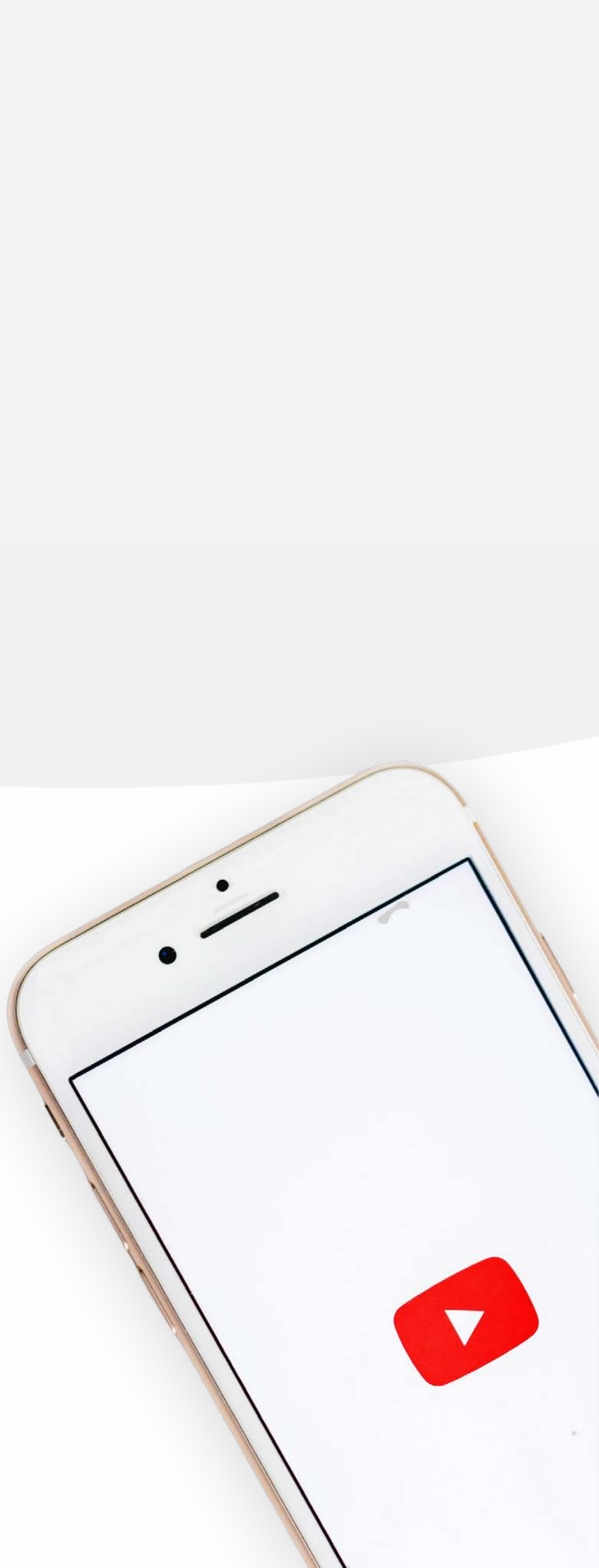
    » The **younger** setting is designed for children ages 5-7. Content available includes songs, cartoons, crafts, and more. Like the above, not all videos are manually reviewed, so you might come across inappropriate content, though it isn't likely. You can also turn the search function off if you don't want your child to potentially find something you don't agree with.

- The **older** setting is designed for children ages 8-12. Since it's aimed at slightly older kids, the content opens up to include music, gaming, and science videos. With this option, search results are limited to videos recommended for kids 12 and under. Though, as above, the search feature can be switched off.

- With **'approve content yourself'**, your child will only be able to do anything that you've approved yourself. This includes collections, YouTube curated lists centered around a particular topic, such as science or music. With this setting, your child won't be able to search.

Whichever you choose, the option is only applicable to that particular profile. So if you have multiple children to set up, you will have to go through one by one. You can add up to eight profiles by selecting the **add** option and completing the same process again. Once completed, select the **arrow** to finish the setup.

As we said, this version of YouTube is much more agreeable than the standard version. If they're young enough, your child won't even notice the difference. Given the variety of content available on the main platform, using a more restricted version is going to save your child from having to see some wildly inappropriate videos.



Some advice to parents on passwords

In 2019, the world's worst password was, 'Password'. It's almost incredible to believe, despite constant advice coming from every angle imaginable, people were still crazy enough to put their whole online lives at risk, by using something as simple as 'Password'. Thankfully, in 2020, there was a new number one for the title of world's worst password. Yes, you guessed it: '123456'. Followed closely by 'qwerty'. Passwords are incredibly important; they're the key to securing all of your online life. They protect everything from your email and social media to your bank accounts. It doesn't help that plenty of people simply struggle to create memorable yet safe passwords. If we can't trust adults to do it right, how will our children fair? For the most part, they're either using their date of birth, 'Password', or something similar. So it's essential that you be the one to take the responsibility for setting their passwords - and making them good ones, too.

You want your child's account to be secure and accessed by nobody other than you and your child. Secondly, they might be too innocently naive to understand why or how to create a complex enough password in line with what we're about to suggest. Thirdly, this allows you to have full access to your children's profiles so you can stay fully aware of their online lives. Outside of these more obvious reasons, we can't expect children to fully appreciate how vulnerable their accounts are to attack; parents themselves struggle with this concept.

Note that this isn't an insult to any children - more often than not, they're more tech literate than their parents. But they don't always necessarily realise how dangerous the world can be.

Children also frequently share passwords with each other. They do this for a myriad of reasons. From a group of children who share a single social media page, to having a friend maintain their profile while going on holiday, to keeping up streaks on Snapchat. Teach your child that they should never share their password with any other person other than their parents or another trusted adult. It's better that a parent creates the account password as it teaches good password etiquette from the very start. Children need to learn that they should never reuse the same password on other platforms. Nor use a default password.

You might also want to consider using a password manager such as Lastpass or Dashlane. They are great for helping you manage all of your passwords, allowing you to create complex ones without worrying about remembering them in the future. If you decide not to use one, then use a mixture of capital letters, lowercase, numbers, and special characters. It's recommended that passwords should contain anywhere between 16 to 32 characters. This is a difficult enough task for an adult, let alone for a child.

The advice in the past has been to change or update your password every three to six months. While this advice is still relevant, if you're creating strong 16- to 20-digit passwords in conjunction with a two-factor authenticator such as Google Authenticator or Authy, the account should be secure. The only reason to change the password is in the event of a data breach where your login credentials are leaked. A recent paper entitled '(How) Do People Change Their Passwords After a Breach?', released by Carnegie Mellon University in the US, revealed that a worrying number of people don't react at all to data breaches. The researchers found that very few of their participants intended to change their passwords, even after being notified that their passwords were compromised or reused. Some stood firm because they believed in the "invincibility" of their passwords. Whether it was an invincible password or a lazy user, in both cases, the account was vulnerable.

Almost more incredibly, one-third of those who did eventually change their password took more than three months to get around to it. Of those that did, many replaced their old passwords with weaker ones. Ultimately, we humans really aren't good at generating the necessary randomness required for creating strong passwords. It seems we aren't very good at reacting to data breach advice either.

How can you create a secure account online for you and your children?:

+ Check if any of your online accounts, or those of your family, have been compromised in a data breach. You can do this by simply entering the email address you use in to this site https://haveibeenpwned.com/
+ You can even test the strength of your passwords on https://haveibeenpwned.com/Passwords. It will tell you whether the password has been leaked in a past data breach, making it an insecure password.
+ Use a mixture of capital letters, lowercase, numbers, and special characters.
+ Use 16 to 32 characters.
+ Use two-factor authentication.
+ Use a password manager and an authentication app.
+ Never write down your passwords where they can be easily accessed.
+ Never store your passwords on your device.
+ Never use default passwords.
+ Never reuse a password you have used previously.
+ Never use the same password on multiple platforms.
+ Change passwords every three to six months, however if you become aware of an account being breached, change your password straight away.
+ Never let children be responsible for creating or maintaining their own passwords.

2

Amazon

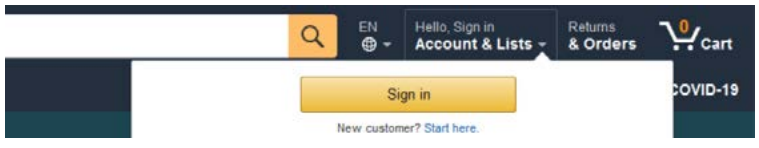
Amazon Echo

Our homes are becoming 'smarter'. The 21st century has been typified by the rise of the 'smart home' with a myriad of devices that can control every facet of your home life. At the top of the list are the smart speakers - gadgets that you can ask questions and talk to. Amazon has their own version - the Amazon Echo. They're handy devices to have around the house, and they come with their own suite of parental controls.

Restrictions available:

+ App access
+ In-app purchasing
+ Online gaming

While they don't have the most extensive range of restrictions, there are a couple of key limits you can impose.



Creating and setting up your Amazon Household account

+ Log into your Amazon account.
+ Under **accounts and lists**, select **your account.**
+ Select **shopping programmes and rentals** and choose **Amazon Household.**
+ Select **add a child** and then enter their details.
+ Click **manage your content and devices** to control what your child can access and purchase on the devices they have access to.
+ Select a **pin code** and **disable voice purchasing** to prevent any unauthorised purchases.

Changing your settings on your smartphone

+ Open the **Alexa app** or go to **echo.amazon.** com on your smartphone and select the **menu icon.**
+ Select **settings** and scroll down to **voice purchasing.**
+ Choose a **4-digit** pin then select **save** to set up the pin. You can disable voice purchasing completely if you wish.

Amazon Fire Tablet

Tablets: we've mentioned them before and they'll come up plenty of times again. Your house will no doubt have at least one of them, if not multiple. While Apple might be the king of the tablet scene, Amazon has released their own version - the Fire Tablet. To set up parental controls on one of these devices, you'll need an Amazon account. Once you have one, you can use the following restrictions.

Restrictions available:

+ App access
+ In-app purchasing
+ Online gaming

Let's take a look at how to make your child's Amazon Fire Tablet safer.

Setting up parental controls

+ To begin, swipe down from the top of the screen and select **settings** and then **parental controls**.
+ On the **parental controls** page, activate by swiping right.
+ You will be prompted to enter a password - confirm the password and select **submit.**

Creating and setting up your Amazon Household account

+ Log into your Amazon account.
+ Under **accounts and lists,** select **our account.**
+ Next, go to **shopping programmes and rentals** and select **Amazon Household.**
+ Choose **add a child** and then enter your child's details.
+ Then select **manage your content and devices** to control what your child can access and purchase on the devices they have access to.
+ Enter a **pin code** and disable **voice purchasing** to prevent any unauthorised purchases.

Changing your settings on your smartphone

+ Open the **Alexa app** or go to **echo.amazon.com** on your smartphone and select the **menu icon**.
+ Select **settings** and scroll down to **voice purchasing.**
+ Choose a **4-digit pin** then select save to set up the pin. You can disable voice purchasing completely if you wish.

Some advice to parents on smartphones

There's no rule, written or unwritten, on when you should let your child have their first smartphone.

Parents are under more and more pressure to provide their children with devices earlier and earlier. While most people generally recognise that children under 7 shouldn't have one, a recent survey showed that a quarter of all 7 to 9 year olds already own one - and this figure is increasing.

Recent studies recommend that children aged 10 to 12 should not have their own internet-enabled mobile devices at all, and that all children under the age of 12 should have daily screen time limits of under two hours set across any devices.

Giving a child of any age a smartphone is an exceptionally serious decision. It's not one that should be taken lightly. In essence, you're deciding whether you want to give them unrestricted access to the online world. What should be at the forefront of your mind while making this decision is that this will now also allow anyone in the world to access your child.

It's really important for parents to fully comprehend this situation. While giving them a phone might seem like the right choice - after all, it allows you to call them wherever they are - that's not the main reason they want one. It isn't about calling people or even messaging them. It's about accessing the online world and all the apps and experiences that go along with it.

It's really important for parents to fully comprehend this situation. While giving them a phone might seem like the right choice - after all, it allows you to call them wherever they are - that's not the main reason they want one. It isn't about calling people or even messaging them. It's about accessing the online world and all the apps and experiences that go along with it. We need to differentiate between what your child is asking for and what you might believe you're giving them. It's also worth pointing out the distinction between a smartphone and a mobile phone. A mobile phone, by which we mean a device without internet access, can be given to a child at any age. They're great in the event of an emergency, if you're going to be late picking them up from somewhere, or to generally just make phone calls. But your child likely won't get this nuance, so if they ask for a mobile, they really mean a smartphone. But we have absolutely no reservation in saying children, while still in school, are neither prepared nor have the level of emotional intelligence, ability for critical thinking, or resilience to be afforded this level of access to the online world.

A smartphone should never, ever be given to a child before they start secondary school, and only then based on their own intellectual capability at protecting themselves online. The decision has to be based on their level of maturity, responsibility, and their assured constant engagement with you about what they're doing online.

Over the years, we've met countless parents who essentially felt bullied into getting a device for their children. If you're still on the fence, hopefully this gives you the perspective you need and reassures you you're making the right choice. Children will always want something that everyone else has. What people have right now is a smartphone. Neither you or your child really have any idea whether all the other children you know are having entirely positive or negative experiences online. Most children are very secretive about it. Many parents only discover something serious has happened after the fact. It's hard to put yourself in that mindframe of "what would you do" if your child was dealing with disrupted sleep, cyberbullying, online sexual exploitation, access to pornography, or technology addiction. It isn't really happening, so you don't know how you would react. But if they were happening right now, how would you deal with it? Does that affect whether you think they're ready to be exposed to that world?

Consumerism can be a hard peer pressure to ignore. There's a level of psychology at play from tech companies who make you believe you need their product. A constant mantra that children will fall behind and be tech illiterate if they can't have the latest iPhone. This is neither true nor valid. Generally, in every home, there are a multitude of digital devices. So that risk of falling behind is non-existent. Especially since, once you know your way around one digital device, you know your way around them all. They're intuitive like that. And with the COVID-19 crisis forcing education online, they're more familiar than ever.

"Consumerism can be a hard peer pressure to ignore."

Parents believe their children will be subjected to bullying if they don't get their child a device. Parents need to be really honest with themselves here. Bullying has always existed and shows no signs of going anywhere for now, despite the best efforts of everyone involved. And online bullying is, unfortunately, no different. The bullying that might take place in school will pale in comparison to cyberbullying. We've met countless students and parents who have suffered through the deep impact it can have on a young life. Bullying in the real world has geographical and physical restrictions. Unfortunately, there are no such restrictions in an online environment. Again, it's hard to put yourself in that spot and imagine it could happen to your child, but the truth is, it can.

Once most children get their smartphone, almost immediately, there's a perceived entitlement that it means they get privacy. We've had plenty of children tell us that their parents don't know what accounts they have, their passwords, or who they're in contact with. What's almost worse is when we meet parents who feel like they're invading their child's privacy by going through their device. We don't hold anything back in our advice to parents here. Children are exactly that: children. They have a very long path of learning ahead of them before they'll have the instincts and foresight to identify potential risks. Some may be easily identifiable, but there are many others that are far more difficult to recognise. Adults, some of whom are technology gurus, often fall prey and become victims to online criminals or extortionists. If knowledgeable adults are at risk, then realistically, what hope does a primary school child have?

You need to be a key part of your child's online life. The alternative is you take a gamble that they won't end up being a victim to one of the multiple possibilities of online harm. It's a far better option to stay fully engaged with your child when they access the online world, rather than permitting them to unwittingly engage with an online predator or cyberbully without your knowledge. Even if the child manages to avoid all avenues of online danger, without that collaboration, children may act inappropriately. So, there are behavioural aspects that also need to be taught to a child to ensure they become safe, positive, and proactive digital citizens, rather than feral internet children.

The only way to appropriately monitor your child's online life is to have that involvement. As stated already, children are exceptionally vulnerable. They need to be taken care of; they need boundaries. The online world needs to be restricted according to their age requirements. You have to be fully informed about who your children are in contact with at all times when they're online. Just like in the real world, where children strictly adhere to specific safety rules that protect them from harm, these rules need to be applied by parents when children go online. Make no apologies at all for this. You're the parent. It's your job to protect your child. Nobody can make you intentionally put your child in danger - nobody would even expect you to do that. It's your choice - your decision - where, when, and how they access the online world. This decision isn't your child's decision, or your other family members, friends, neighbours or any of the technology companies or platforms who are simply trying to sell you their product. It's yours and yours alone.

"The only way to appropriately monitor your child's online life is to have that involvement."

If you've decided the time is right to permit your child to have a smartphone, it certainly helps to clearly set out rules and guidelines relating to online access first. We recommend signing the social media contract from earlier in the book. This clearly sets out what's acceptable, what's not acceptable, and what's expected of them as a responsible user of the device.

3

Apple devices

iPhone and iPad

iOS is a leading operating system for phones and tablets, with Apple's iPhone and iPad having a healthy chunk of the market. So it's highly likely you'll have at least one of them in your home. Thankfully, they come with a wealth of restrictions on using specific features and applications. This includes blocking access to the iTunes Store, restricting explicit content, and stopping in-app purchases. It's also possible to limit the access to the camera and manage any potential image sharing.

Restrictions available:

+ App access
+ Data sharing
+ Internet browser access
+ In-app purchasing
+ Inappropriate content
+ Location sharing
+ Online gaming
+ Social networks
+ Streaming media

So how do you access these options and what do we recommend?

Setting up parental controls

+ Using the **screen time** option, you can set up **content privacy restrictions.**
+ Go to settings and select **screen time.**
+ Select **continue**, then choose **'this is my device'** or **'this is my child's device'**.
+ If you're sharing the device and want to ensure your settings aren't changed, you'll need to activate the **screen time passcode,** enter a passcode, and then re-enter it when prompted to confirm.
+ If the device belongs to your child, follow the prompts until you get to the **parent passcode,** enter one in, and then re-enter it when prompted to confirm.
+ Now select **content and privacy restrictions.**
+ When prompted, enter your **passcode** - now you can activate the **content and privacy** features.

+ Here you can manage **in-app purchases, apps allowed,** and **content restrictions** which can be used to set age-rated specific content.
+ You can also set up privacy settings for the device and the apps installed.

iTunes and App Store purchases

+ Select the **iTunes and App Store purchases** option.
+ Here you can choose which setting to apply to **installing apps, deleting apps** and **in-app purchases**. We advise setting it to don't allow or always require a password for younger children, so they'll always require your permission to add or remove any apps from the device.

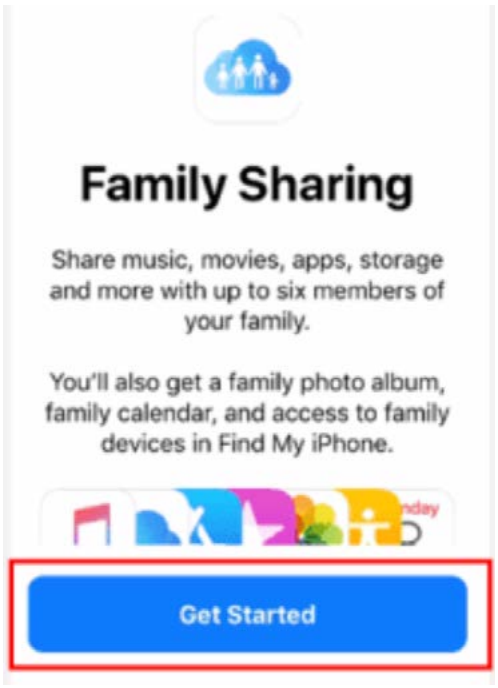
Family Sharing

Tech giants like Apple understand that a household might have more than one of their devices. So, to provide a helping hand, they've included a Family Sharing option to make it easy for families of up to six people to share music, movies, TV, shows, apps, and other Apple Store purchases. All while everyone still has their own independent account - and even using just one credit card. It's a neat little feature that makes it simple to share purchases and even photos and a calendar. For parents, it's just what you need.

Restrictions available:

+ App access
+ Inappropriate content
+ Time limits
+ Privacy
+ In-app purchasing
+ Streaming media
+ Parental control
+ Location sharing

But there's nothing on the device to compel you to do it, potentially leaving you scratching your head about how to set it up. To make your parenting life easier in the future, let's run through how it works.



Getting started

It's worth noting that you can only be a part of one family at a time. Something to keep in mind if you have a two-household family. To set up **Family Sharing:**

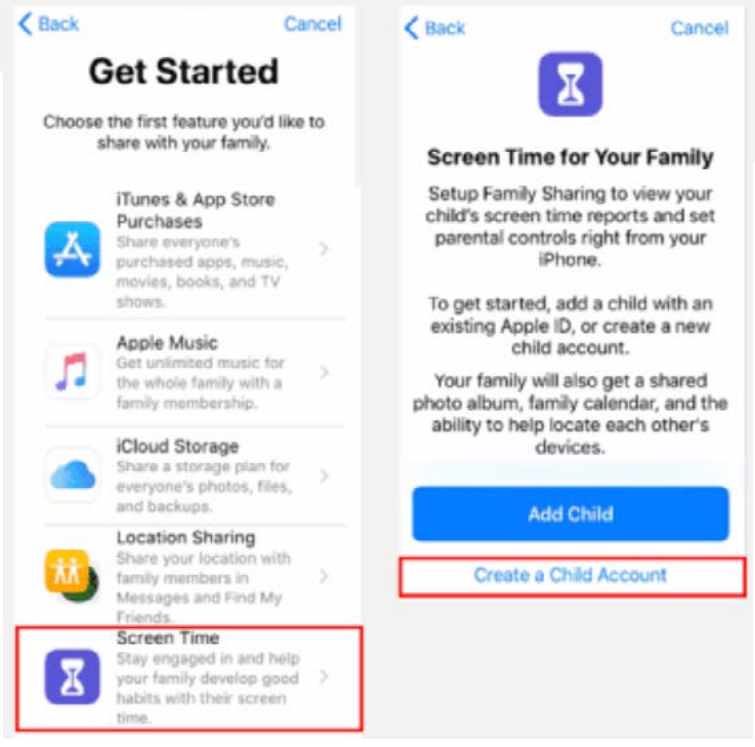
+ Use an **Apple ID** signed in to **iCloud** and **iTunes** on an iPhone, iPad, or iPod Touch with **iOS 8** or later, or a Mac with OS X Yosemite or later.

+ If you need to, you can create an **Apple ID** for your child, then add them to your family group by selecting **add family member.**

Age verification
Before you begin, make sure you're using a supported payment method. You can check your payment method from your **Apple ID** account page or in **iTunes.**

To comply with child online privacy protection laws, you use the **CVV,** verification code sent via SMS, or security code from your payment method as part of providing your verified parental consent. If you don't have a supported payment method on file, you'll be asked to change it to one that is.

After you create the child's **Apple ID**, you can change back to the original one. We would strongly advise you not allow your children to make any purchase online without parental knowledge and consent.



Setting up an Apple ID for your child
If you want all of the family to be able to access Family Sharing, they'll have to have their own Apple ID. Since children under 13 can't create one on their own, Family Sharing allows you to do it for them. This way, they'll be able to use iCloud, iMessage, FaceTime, and any other apps they'll likely want to use.

On the off chance your child already has an Apple ID, you can still easily add it to the family group and change any details as you see fit. But if they don't, it's a simple enough process.

Creating an Apple ID for your child
+ Using **iOS 10.2** or earlier, go to **settings,** then **iCloud**, then **family**.
+ For all other versions, go to **settings,** then **[your account], set up Family Sharing, add family member, create a child account,** and finally **next.**
+ Enter your child's birthday and select **next.** While it's important to be sure to enter the correct year of birth, we do advise that you select a different day and month so, in the event of a data breach, the child's actual date of birth isn't exposed.
+ Review the **Parent Privacy Disclosure** carefully before proceeding.
+ Enter your payment information and select **next.** If you don't have one on file, you may need to add one.
+ Enter your child's name, then select **next**.
+ Now create your child's **Apple ID** (username@icloud.com) and select **next.** Again, privacy should be considered when creating a username. We recommend not using the child's actual name, rather something easily remembered but unconnected with the child.
+ Follow the instructions to set a password, choose security questions, and set up your child's account. Go back to our section on creating a password for advice on what to pick, just make sure it's something you can remember.
+ You can decide if you want to activate the **ask to buy** option, which will approve all iTunes, Apple Books, and App Store purchases made by your child. **You will be responsible for all charges to your account.** Once you have decided, select **next.**
+ Fully review the terms and conditions before selecting **agree.**

Starting a family group
To start Family Sharing, one adult has to become the 'family organiser'. They'll have the power to add people to the family group and switch on certain options, such as purchase sharing. It's not complicated to get started though...

The first steps

+ If you're using **iOS 10.2** or earlier, go to **settings** then **iCloud.**
+ For any version after that, go to **settings** then **[your account].**
+ Now select **set up Family Sharing.**
+ Select **get started.**
+ Follow the instructions to set up your family group and add your family members.
+ If you're using **iOS 11** or later, choose the first feature you'd like to share with your family. Then follow the instructions to invite your family members using **iMessage.**

How to add a family member

+ If you're using iOS **10.2** or earlier, go to **settings,** then **iCloud**, then **family.**
+ For any version after that, go to **settings,** then **[your account]**, then **Family Sharing.**
+ Select **'add family member'.**
+ Enter their name or email address.
+ If you're using **iOS 11** or later, choose whether you'd like to invite them via **Messages** or do it in person. Then, for whichever you pick, follow the onscreen instructions.

If they're with you, they can enter their password themself to accept the invitation. You can also link to their device and send one over to accept. We recommend you set all this up yourself and accept it on your child''s device to speed up the process. Once you've accepted the invite, you can hand it back to your child knowing everything is ready to go.

Setting up Screen Time

+ Go to your **settings**, then select the **Family Sharing** option.
+ Find the **Screen Time** option and choose which child you want to set it up for.
+ Follow the onscreen instructions and select what time the device will be active. The **downtime** section shows you when the device will be inactive and unusable by your child.

How to disable in-app purchases and downloads

+ Following the instructions above, return to the **Screen Time** menu.
+ From here, find the option for c**ontent and privacy restrictions.**
+ Next, go to **iTunes and App Store purchases.**
+ Here, you can also block their ability to **install apps.**

Setting up app limits

+ Here, you can set up daily time limits for all of the apps your child uses.
+ The Apps are arranged in categories which makes them easier to identify.
+ Select the specific app categories you're looking for then select the **set app limit** option

Apple HomePod

The Apple HomePod is the company's version of a smart speaker. It's an audio hub for your house, and together with Apple Music and Siri, it becomes an extremely convenient way to bring your home to life with some music. Beyond that, it can actually help families with everyday tasks, such as asking for the weather or putting together a shopping list. Anyone can control it with their voice and use it to access whatever content they need. And this includes children. So making sure to enable parental controls is essential; to do so requires an Apple ID.

Restrictions available:
+ App access
+ Streaming media

Most of the restrictions you can impose can be done through Family Sharing, so check that chapter for more details. But something specific to the HomePod is streaming explicit music.

Disable explicit content
+ On your iPhone or iPad, open the **Home** app.
+ Find your **HomePod** and press and hold on it.
+ Next, select **settings.**
+ Under the **music and podcasts** heading, you can **toggle off explicit content.**

4

Google

Google Family Link

Google is the undisputed king of the technology world. We can guarantee you use their services in some way, be it through their search engine, Android OS, or email service. They're so pervasive that it's almost impossible to avoid them. Thankfully, they have a solution perfect for every parents' needs.

Google Family Link is a free app available in both the Google Play Store and Apple App Store which can be installed on any Android or iOS device. With it, you can set specific digital rules on your child's devices. It has a wide variety of options, ranging from managing app access to limiting screen time and viewing browser history. It's even possible to cut off the device remotely - say, at bedtime. The capability is there for you to help your child develop a healthy relationship with the online world and teach safe habits. To get started, you'll need a parent Gmail account and one for your child.

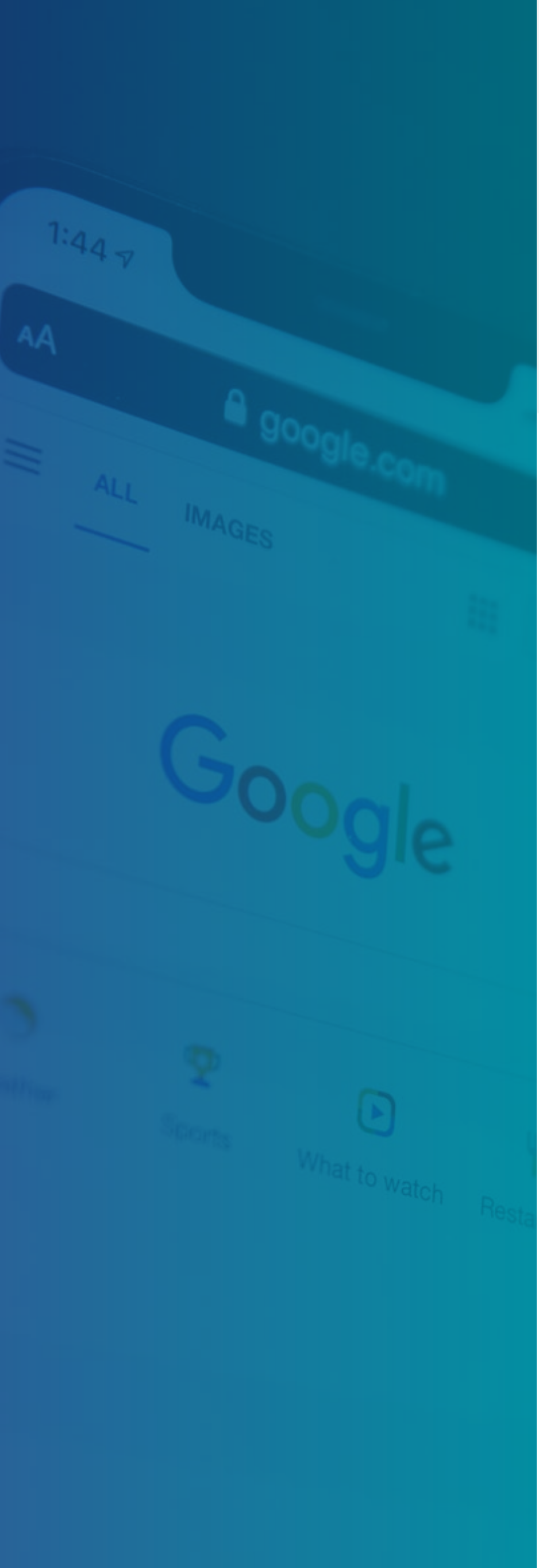
Restrictions available:

+ App access
+ In-app purchasing
+ Internet browser access
+ App blocker
+ Inappropriate content
+ Location sharing
+ Streaming media
+ Time limits

Before installing Google Family Link, ensure both your device and your child's device are compatible. Also make sure that your device is running either Android **Nougat 7.0** or **Marshmallow 6.0** (or above). You can check this on your device by opening settings, then scrolling down to the bottom and selecting the option **'about phone'** or **'about tablet'** to see the current version of software the device is running on. You may have to update it if your device is behind. It's good practice to always have the latest version of your operating software running on every device as this guarantees it will work with the most recent apps and has all the updated features you need.

Setting up Google Family Link

+ Download the **Google Family Link app** from the respective store on your parent device and your child's device.
+ A code will be displayed to enter on the child's device once you have installed Google Family Link. This will link the devices.
+ You will need your own Gmail as a parent account. If you don't have one, you'll need to set one up. It's fairly simple and self-explanatory to do. To confirm the account as an adult one, you'll have to enter your bank card details. There'll be a nominal charge applied to the card, which will be returned. The child will not have access to the card or be able to make purchases using the bank details you enter.
+ Once you have your account set up, it's time to **create your child's account** by entering your child's name, their date of birth, and their gender. We always advise using incorrect information, never the actual details of the child or their date of birth. Only the year is of importance.
+ Create an **email address** and **password** if one does not already exist.
+ Confirm your parental consent by entering your card details.
+ Now **connect your child's device** to Family Link. This step can take anything up to 15 or 20 minutes.
+ If your child's device is compatible, you shouldn't run into any issues, but be sure to check beforehand at the beginning of the installation. Older models may not support Google Family Link.



+ If the device is a shared device, you will have to either create a new user on the device or delete the existing users to set up the app.
+ **Log into the app** on your child's device using your child's **email** and **password.**
+ Select your account to set parental permission.
+ You may need to repeat this procedure if there's more than one child account required.
+ Name your child's device and review what apps are installed on the device. You can choose which ones your child has access to on their device.
+ Once completed, you'll be able to customise your child's settings through Family Link on your own phone by selecting the name of your child.
+ Select **choose settings** to set up parental controls and filters across the range of apps on all of your children's devices.
+ It's possible to use Google Family Link to monitor your child's location. To enable this feature, select **set up** in the **location** menu and select **turn on** to see your child's location.
+ On the app **activity** menu, select **set up** to monitor which apps your child is using and for how long.
+ Here you have the option to set daily limits on your child's device. To use this feature, select **edit limits.** Limits can be applied individually to each day of the week and will cut off after the time specified.
+ Using the **edit schedule** feature, you can set a bedtime which will cause your child's device to shut down.
+ It's recommended that you also use additional software to restrict access to the **settings menu** and the **Google Play Store.**

Google Home

Google Home doesn't have any parental controls. However, it is possible to limit what can be played and searched on Google Play Store and YouTube. Users require a Gmail account.

Restrictions available:

+ Inappropriate content
+ Media streaming

Here are a couple of suggestions for what you should change.

Restricting explicit YouTube videos

+ Open the **Google Home app.**
+ Open the **menu** and select **devices.**
+ Select your Google Home from the list of available devices.
+ You'll see the heading **YouTube restricted mode**. Slide the toggle button to the right to block restricted content.

Restricting explicit songs on YouTube Music

+ Open the Google Home app.
+ Select the **settings** option from the menu.
+ Under the **features** heading, select **digital wellbeing.**
+ Choose your device. Under **music**, select whether you want to block explicit music or all music.

5

Android Devices

Android smartphones

As popular as Apple is, the market is dominated by Android. Did you know that Android phones account for almost three-quarters of all smartphones? This might be a shock, but it's true. The chances of you having one in your house are quite high. But parental controls aren't handled by the device itself, but through Google Family Link. To set this all up for your child, they'll need a Gmail account and password. This can either be their own or simply just used yours.

If you're using WardWiz Android Essentials, you can lock the Google Play Store completely, which ensures you can speak with your child and review any app before it's downloaded onto the device. If you don't quite want to go to that length, there are some restrictions available that you can access through the Play Store itself.

Restrictions available:

+ App access
+ In-app purchasing
+ Online gaming

Without any extras, there are a handful of changes you can make through the settings.

Google Play Store parental controls

+ Open the **Google Play Store app.**
+ Swipe right and select the **menu.**
+ From the menu, scroll down and select **settings.**
+ Scroll down and select **parental controls.**
+ To activate them, swipe the toggle button to the right.
+ You'll be prompted to create a **PIN code.**
+ From here, it's possible to set age-gated restrictions for apps, games, films, TV shows, magazines, and music.

App purchases (including in-app)

You can also set it so Google asks for the account password when making any purchases.

+ Open the **Google Play Store app.**
+ Swipe right and select the **menu.**
+ From the menu, scroll down and select **settings.**
+ Scroll down and select **require authentication for purchases.**
+ On the **require authentication** pop-up window, you can set it so authentication is needed for **all purchases, every 30 minutes after entering your password**, or **never.**

Installing applications from unknown sources

It's important to block devices from being able to install applications from services other than the Google Play Store. Apps downloaded from unknown sources may contain malicious content which can be harmful to the device and could pose a risk to its security and integrity.

+ On your device, swipe the screen down and select the **settings.** It may look like a small cog icon.
+ In the **settings menu,** scroll down and select the category about **apps and notifications.**
+ Find the option for **installing unknown apps.**
+ Ensure that the toggle switch is set to off for each app. This stops them from downloading and installing unknown apps.

Android tablets

Just as there are iPhones and iPads, there are Android phones and tablets. But unlike the Apple products, Android software runs on a number of companies' hardware, including Google and Samsung. Much like the phones, there aren't many parental controls built into the tablets, meaning you'll have to rely on Google Family Link to do most of the heavy lifting. Check the Google section of the book for more information on setting that up.

Restrictions available:

+ Parental controls

Similar to the phones, there are some changes you can make.

Setting up parental controls

+ To begin, swipe down from the top of the screen and select the **cog icon** in the top-right corner to open the **settings menu.**
+ Scroll down through the menu and select **users.**
+ Add a new user by selecting **restricted profile.**
+ You will then be prompted to set up a screen lock and password to protect your apps and personal data.
+ Select from one of the three security options: **pattern, PIN, or password.**
+ You will then be prompted to complete the profile information of the new account user.

Samsung smartphones

While Samsung phones use an Android-based OS (operating system), it's a heavily modified version, meaning Samsung phones have their own distinct quirks. After iPhones, Samsung's models are the most popular ones around, so you're likely to run into one at some point. Thankfully, they come with their own suite of parental controls; again, they work best in conjunction with Google Family Link.

Restrictions available:
+ App access
+ Online purchasing
+ Internet browser access
+ Time limits

As Samsung's differ from your average Android phone, let's walk through how to adjust the settings.

Reviewing your child's internet browser history
+ Launch the **browser app.**
+ Select the **bookmark** option.
+ Select the **history** option to view what your child has been looking at.

Setting up Secret Mode
Today, most browsers have an anonymous browsing option that allows the user to search the internet without it leaving a trace in their history. Any savvy child will know this is how they can hide searches from their parents. But with Samsung, you can lock this option away.
+ Launch the browser app.
+ Select **tabs** in the top-right corner of the screen.
+ Select turn on **Secret Mode.**
+ If this is the first time selecting this option, the device will ask you to set up a password. Choose one you'll remember using our advice earlier in the book. From now on, to use the feature, your child will have to enter a password.
+ In the case you don't enable this option at this point, you can still access it in the settings - look for the privacy and security section.

Setting up a secure folder
Secure folders are often used by children to hide content, contacts, and apps from their parents. Similar to Secret Mode, you can set this up with a password they don't have access to. Once the secure folder is created, they won't be able to set up another one. For older children, we recommend they share this password with you if they're using it so you can monitor its use and content.
+ Go to **settings**. From there, go to **lock screen and security.**
+ Scroll down and select **secure folder.**
+ You'll be asked to select a **PIN.**
+ The secure folder is now set up.

Samsung tablets

Similar to phones, Samsung's tablet offering is a popular choice after Apple's iPad. And just like Samsung's smartphones, there are some parental controls available to you.

Restrictions available:
+ Internet browser access
+ File sharing

Our advice for what restrictions you need are the same as our recommendations for the smartphones, but we're including it here again for simplicity's sake.

Reviewing your child's internet browser history
+ Launch the browser app.
+ Select the **bookmark** option.
+ Select the **history** option to view what your child has been looking at.

Setting up Secret Mode
Today, most browsers have an anonymous browsing option that allows the user to search the internet without it leaving a trace in their history. Any savvy child will know this is how they can hide searches from their parents. But with Samsung, you can lock this option away.
+ Launch the browser app.
+ Select **tabs** in the top right of the screen.
+ Select **turn on Secret Mode.**
+ If this is the first time selecting this option, the device will ask you to set up a password. Choose one you'll remember using our advice earlier in the book. From now on, to use the feature, your child will have to enter a password.
+ In the case you don't enable this option at this point, you can still access it in the settings - look for the privacy and security section.

Setting up a secure folder
Secure folders are often used by children to hide content, contacts, and apps from their parents. Similar to Secret Mode, you can set this up with a password they don't have access to. Once the secure folder is created, they won't be able to set up another one. For older children, we recommend they share this password with you if they're using it so you can monitor its use and content.
+ Another option is to know your child's password to their secure folder
+ Go to **settings**. From there, go to **lock screen and security.**
+ Scroll down and select **secure folder.**
+ You'll be asked to select a **PIN.**
+ The secure folder is now set up.

Samsung Family Hub

Smart technology is more prevalent in homes than it's ever been. From smart TVs to smart speakers, you're never far away from a smart device. One such piece of tech is the Samsung Family Hub refrigerator. Yes, a refrigerator.

Any device that connects to the online world needs to be secured - even a refrigerator. The novelty of these devices often come before the security aspect. Please take a moment to ensure even these most basic steps are taken to ensure you and your family are protected.

Restrictions available:
+ App access
+ Online purchasing
+ Internet browser access
+ Time limits

Here's how you can adjust the settings on your fridge.

Setting up security controls on the Samsung Family Hub
+ Begin by opening the **settings** from the home screen.
+ Now select the **security** option from the items displayed.
+ Choose **enable restrictions.**
+ If this is the first time accessing this, you'll be prompted to set a 4-digit PIN.
+ Confirm by re-enter the pin.
+ Now is a good time to review the available widgets on the device and choose which ones will require a PIN to access.

Some advice to parents about online privacy

It's a harsh and sad truth that the legal term "volenti non fit injuria" - "To the consenting, no wrong is done" - can easily be applied to social media platforms, or indeed anything you or your child willingly downloads and installs. When you strip the term down, it means when someone willingly places themselves in a position of potential harm, knowing that something might happen, where they can't then blame the other party 100%. The attitude is that they knew the risks, so they can't complain when there are consequences. Despite talking about children here, the rules still apply. We've all slipped up online. How many terms and conditions have you agreed to without really reading them? Theoretically speaking, once you click accept, you or your child are acknowledging that you have fully read the terms and conditions and accepted them to use or access the platform or application.

However, whether you've read them or not doesn't matter. You agreed either way. Those terms, conditions, and permissions you accepted may be far more costly than you may think.

There's an old saying: "If you're not paying for a product, you're not the customer - you're the product." This sentiment has never been truer. The vast majority of content available for download and use on digital devices today is free. The meaning of free being, it's free, but it will cost you. That cost, in the majority of cases, is unlimited access to your personal information. Data is the new

black gold. Humans are producing more of this than ever before, which is being harvested through digital devices and sold on to third parties for a variety of reasons. One being the ability to target advertising specific to you.

There's little point in attempting to sell shampoo to a bald man. However, knowing the man is bald affords the opportunity to sell him a hat, especially if the bald man lives somewhere very hot or cold. Knowing where you live, where you go, who you interact with, what you like, what you don't like, your sex, age, political leanings, religion, or sexuality means companies know you better than you even do yourself. And all of this data comes directly from you, through your own interaction with your ever-present digital device. Many people feel very uncomfortable when they realise all the free content they installed on their device wasn't free at all. Discovering you've paid for the service through intrusive monitoring of your on- and offline life can be a little unsettling. However, this isn't half as unsettling as realising your child is also subject to the same level of intrusion.

We frequently see parents innocently hand their devices to children in an attempt to keep them quiet while enjoying a family meal. When they get their hands on it, they download every brightly coloured app aimed at children going. Again, all done fairly innocently. But those apps aren't innocent. When you get your device back, it's possible it's not only hoovering up all your data, but may contain a key logger or webcam hack. If they download apps from a less-than-reputable source, it can carry plenty of dangers with it. Not ever Google Play or the Apple App Store are immune from hosting malicious apps.

Over the last few years, thousands of apps have been removed after concerns have been raised by victims who downloaded them. It might have been sitting in the store for months, in some cases years, before people realised how harmful it was. You may only discover this for yourself after your bank accounts are affected. We have to start paying far more attention to what potential risks we are placing the whole family in every time we accept terms and conditions and install content onto our digital devices. It's why we recommend you install some form of antivirus protection across your devices and those of your children.

The reality of just how much personal data can be misused has only begun to be exposed. The Cambridge Analytica scandal momentarily focused people's attention on Facebook. But while we all judged Facebook for playing their part, everyone missed the point that every single application we install is potentially doing the same - if not worse. At present, no one can say for certainty how the invasion of privacy we have accepted in trade for free content will impact us and our children well into the future. However, if what we know from how Facebook has misused the data of its customers, the future looks fairly bleak.

Consider this from your child's perspective. How much valuable personal information and data will an average child create from the time they first use a digital device to the time they reach adulthood? It's frightening to consider how that information could be used by unscrupulous individuals and multinational companies to take advantage, manipulate, or even control someone. It's even more frightening when we realise this is happening already. Insurance companies have been found to have purchased personal data in an attempt to leverage higher payments on those who are inactive. In Ireland, in December 2019, an Irish politician highlighted how motor insurance companies were monitoring customer social media accounts. For anyone who had posted images of themselves abroad, a higher premium awaited them the following year. Why? If a person could afford a foreign holiday, they could afford a higher car insurance premium.

The larger the digital footprint we create, the more it informs those who harvest our data. What we like, who we interact with, and where we go all enable a level of monitoring that makes George Orwell's 1984 look like amateur hour. Unless adults begin to see the potential for abuse, children haven't a hope. Children are entitled to the protection of their data. However, the digital age of consent has been manipulated in this environment, to some degree. While it does afford some protection to young people, the harsh reality is that many parents don't actually know what their children have signed up for. If the digital age of consent is 13, yet the 10, 11, or 12-year-old child has simply clicked through all the terms and conditions to access the game, can it be said they gave their informed consent?

We've met many parents who shy away from the responsibility of making the decisions when it comes to protecting their children online. For

the sake of five minutes' peace, they give in and let a child sign up for an account, or access content, even though the parent will have no idea what it involves. This puts both the parent and child at risk. These risks are not immediately obvious; indeed, the potential harm may not be experienced for some time to come. However, a failure to act responsibly now - to ensure the protection of the child's rights, welfare, and wellbeing - will set the ball in motion for future exploitation of your child's data. Parents can't be expected to read through 10,000 words of legal mumbo jumbo for every application. However, they can look to see what permissions the app wants before anything is installed.

For example, your child wants to download a puzzle game, but it needs access to the device's internet browsing history, contacts, call logs, and text messages. Does that match up for you? Of course it doesn't. But unless we review the permissions, which involves scrolling all the way down to the bottom of the screen where this information is usually kept, nice and out of the way, we won't realise. Choosing to ignore the permissions also brings the risk of the data being exposed in a data breach. Data breaches happen all the time, so it's not a matter of if your data will be breached, rather when. If we combine the reality of data breaches with how careless most people are with what they send and share in what is perceived as a private online environment, then you're looking at a catastrophe for countless people when a breach happens.

Once again, looking at it from a child's perspective, they have absolute trust in this technology. They genuinely have no concept of how insecure their activity is. We can't truly expect them to monitor their own online behaviour from the moment they begin using digital devices. Like us, they'll make mistakes. But unlike us, their mistakes are digitised and may last forever. It's only when we realise how truly vulnerable we are when using this technology that we have some concept of how insane it is to hand a child a device and permit them to journey into a personal privacy oblivion alone. No child should be left to do that. Until we can fully understand the consequences ourselves, children need to be monitored by their parents to ensure they're protected in the years to come.

With the launch of the iOS14 update for Apple devices, they introduced a new privacy-based feature. From now on, the user will be notified if an app is harvesting data from their device.

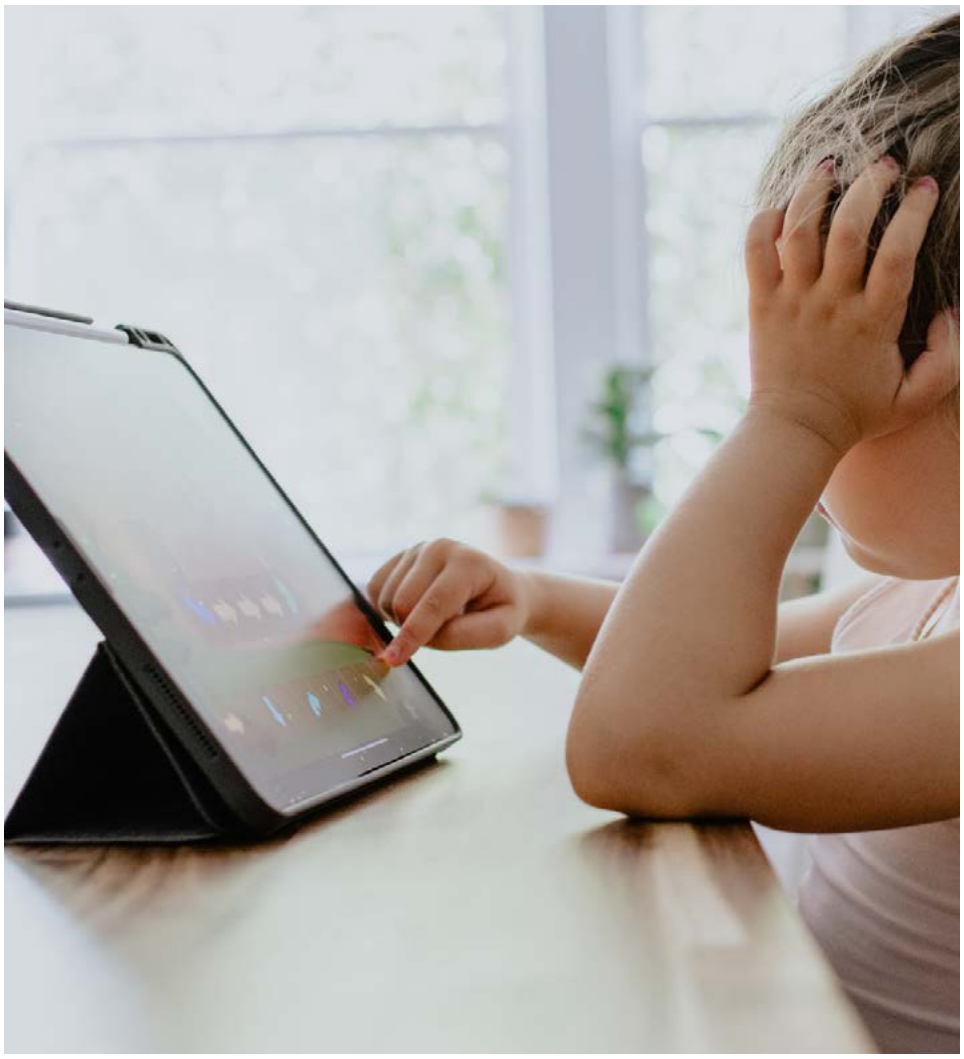
Ben Wood, Chief of Research at analyst firm CCS Insight, said of the change: "Apple's stance on privacy is becoming one of the things that sets it apart from other platforms. It's no surprise that it's pushing its credentials in the area so hard, and making privacy a feature rather than an afterthought."

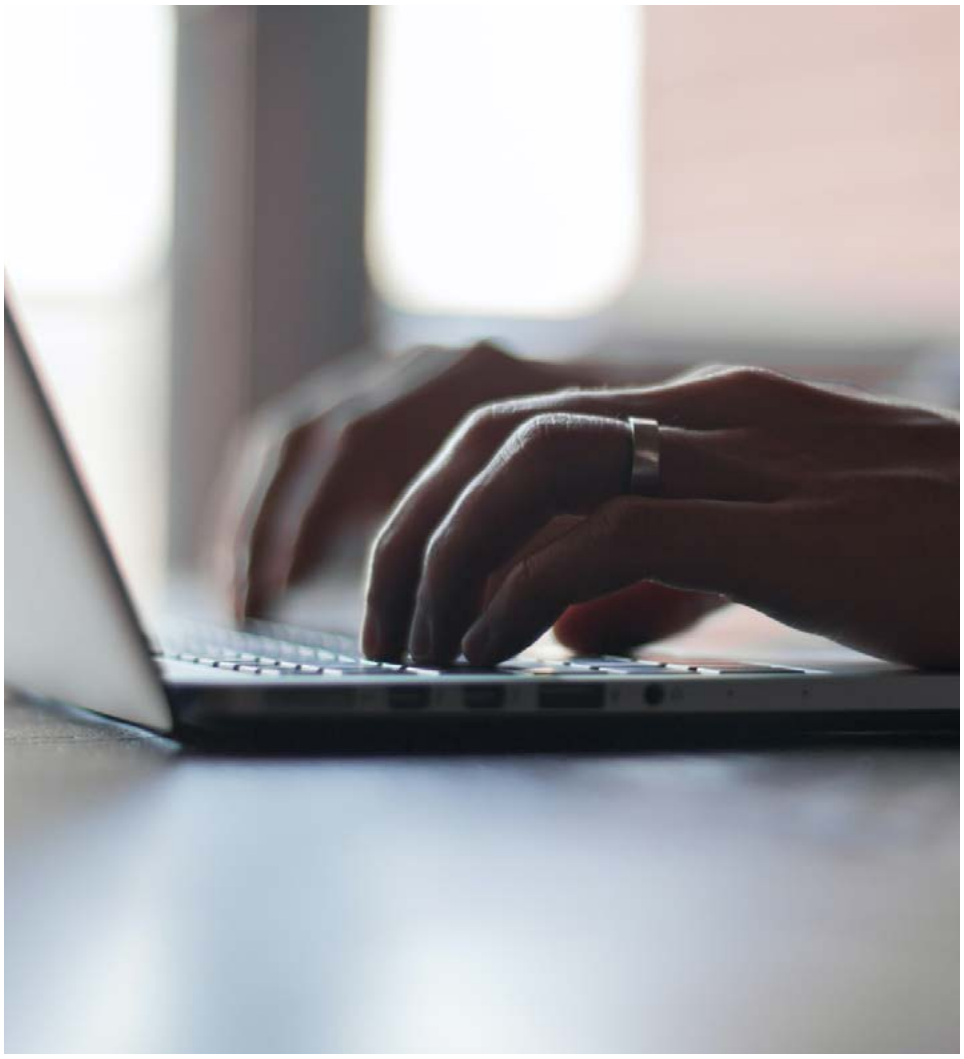
Unfortunately, it seems your ability to protect your privacy might be based on your ability to afford the technology to protect it. Apple devices are not inherently cheap. However, paying a little more to protect both your personal data and that of your children may be worth it in the long term.

Apple has made privacy a company mantra and has set out its four central data privacy principles: data minimisation, on-device intelligence, security protections, and transparency and control. It has declared customers' privacy as a "fundamental human right". With this in mind, the iOS14 update includes a new measure which will require all developers to provide a summary of an app's privacy practices and the data it collects, to be displayed before the user starts a download. Apple likened the measure to "nutrition labels" displayed on food packaging, designed to provide simple-to-read, easily digestible information about a product. Apple's privacy labels will highlight the types of personal data it takes and shares with Apple, as well as the data that could also be delivered to third parties.

The way Apple handles location data is also to be completely overhauled. Users will now be given the option to share an approximate location with an app (coarse location), as opposed to their precise location (fine location). In a move that's well overdue on every platform, from now on, apps that want to track a user's activity across services owned by other companies will be required to ask for explicit permission. The iPhone's status bar will also notify users if an app is using (or has recently used) either the camera or microphone. This has caused some controversy in the past when it was discovered that cameras were being used without the user's knowledge to assess how satisfied they were with a purchase they made on Amazon.

There's a long road ahead of us before we truly know the true harm caused by data harvesting. Until then, we should make every attempt to protect children's digital footprint and personal data.





6

Streaming services and smart TVs

Over the last few years, there has been a huge shift in how we access entertainment on TV. Gone are the days where people were limited by a schedule and lack of time. No more setting up the VHS to record your favourite show, because if you miss the next episode, who knows if you'll ever get to see it. The arrival of downloadable content, streaming services, and the ability to binge entire box sets has dramatically changed what was traditionally seen as a time when the whole family would sit together. This has impacted the whole dynamic of how families interact with each other. Now, a kid can watch their favourite content in one room while mum and dad are watching their choice in another.

" Binging TV endlessly for hours upon hours has also given rise to mental and physical health concerns."

While there are some obvious benefits - such as not having to sit through endless advert breaks or the sheer convenience of it - there are a number of negatives you need to be conscious of. Having everything available at the press of a button means that content orientated towards a more mature audience is now all too accessible to children. Binging TV endlessly for hours upon hours has also given rise to mental and physical health concerns.

YouTube has become the channel of choice for many children and teens. Unfortunately, the amount of inappropriate content they can be exposed to, even with content filters applied, is enormous. Services like Netflix, Amazon Prime, NowTV, Disney+, and many more host content for all age demographics. We frequently meet very young children who are regularly accessing adult content at home. Children openly discuss how they have endured many sleepless nights as a consequence of what they've - sometimes unwittingly - seen. Many will tell us there are actually no parental controls set up or an older sibling or parent gave them the password to access the platform.

We cannot stress enough how important it is to protect children from exposure to adult-orientated content. Sometimes, we take these streaming services for granted, with a somewhat misguided approach of thinking our child wouldn't look at something like that. The cruel reality we've encountered - and this comes directly from young children themselves - is that once one child tells everyone they've seen something inappropriate, it becomes a badge of honour that everyone wants to do. This peer pressure pushes them into watching content they usually wouldn't and definitely shouldn't have seen.

Even if they aren't pressured into it, children can still frequently accidentally stumble onto adult content on these platforms. Curiosity might get the better of them. Or maybe they feel they're mature enough for it. Always remember that viewing inappropriate content can cause severe anxiety and distress in children. It can also negatively impact their wellbeing and long-term psychological development depending on how severe the content is.

It doesn't take a lot of effort to set up parental controls for these platforms. The only way to ensure your child isn't exposed to harmful, disturbing, or inappropriate content is to sit down and set up profiles for them. Make sure they only have access to age-appropriate content. Age ratings afford parents an idea of which audience the content is designed or created for. Use this as a guide to create the level of access you're going to grant the child.

"It doesn't take a lot of effort to set up parental controls for these platforms"

The following services have parental controls: **SkyQ, Netflix, NowTV, YouTube Kids, All4, BBC iPlayer, ITV Hub,** and **Twitch**. While no content restriction or filter is 100% effective, it's imperative to use them to protect your child against exposure to anything harmful. Once the parental controls are enabled, don't give in to a child's request to just see this one show everyone is watching. This can often become the slippery slope which leads to the decline of all the good you have done in setting up the parental controls. Parents need to stay vigilant; ensure your children are only accessing their profile and not yours. You can secure your own profile with a PIN if needs be.

There's no one quick fix to protect your children from exposure to harmful content on all the digital devices in the home. It takes time to set these controls up, but don't become disheartened by the time and effort it requires. At the end of the day, you're protecting your child, and for now, you're the only one who can do that.

Monitor TV time along with screen time for all devices used in the home. Limiting the number of hours they view screens during the day is really important. Take the time to incorporate parental settings on all devices. You should also regularly talk to your children about the content they have seen. Unlike satellite or terrestrial TV, which have specific standards regarding the types of content they can broadcast and specific times for which content can be broadcast, there are no such restrictions in the online world. There are no rules or guidelines. This is what makes it particularly dangerous for children. In a world where anyone can be who they want to be, or share their views or content without restriction, children are frequently exposed to what they may believe are popular children's characters, but have been edited to include pornographic or extremely violent content. Try to watch TV as a family if at all possible. Not as a group of individuals scattered around throughout home, all having an isolated experience with digital devices. Family time is really important. Don't lose it.

All 4

For many TV broadcasters, the shift to streaming was inevitable. Channel 4 - with its range of original broadcasting such as Come Dine With Me, Hollyoaks, and The Great British Bake Off - is one of the UK's biggest channels and has made that jump successfully. Today, All 4 is the umbrella website for their various channels. Even though they don't have much content for kids, they still have some parental controls available. These are restricted by a PIN and come with two options: restrictions for under 16 years and under 18 years.

Restrictions available:

+ Inappropriate content

While limited, there are still parental controls to set up.

Setting up parental controls

+ Open www.channel4.com
+ Select **sign in to My4** in the menu.
+ If you don't already have an account, select **register** and follow the on-screen instructions using your email address and creating a password.
+ Once registered, enter your **email address** and **password** to sign into your account.
+ Select **parental controls** at the top right of your screen.
+ When prompted, select **all rated content 16+** and/or **rated content 18+ content.**
+ You will need to enter a **4-digit PIN.**
+ **Confirm** you agree to the terms and conditions by ticking the option.
+ This will enable the **4-digit PIN** which will now be required to view any content rated above the restrictions selected.

Amazon Prime Video

When it comes to online shopping, no one can beat Amazon. And with free next-day delivery with an Amazon Prime membership, it's all too tempting. For some years now, that membership also comes with access to Prime Video - their streaming platform full of classic and original content, much of it inappropriate for children. To set up parental controls for Amazon Prime Video, you will obviously need to be registered and subscribed to the service. If you aren't, then you don't need to worry about your child accessing this content. The available settings afford parents the ability not only to restrict content based on age, but also on individual devices.

Restrictions available:

+ In-app purchasing
+ Inappropriate content

There are a few restrictions we suggest setting up.

Setting up parental controls and viewing restrictions

+ Go to www.amazon.co.uk and select **sign in.**
+ If you haven't already created an account, select register.
+ Once you've done that, or if you already have an account, sign in using your details.
+ Go to your account page and select **your Prime Video.**
+ Click the cog icon at the top-right and select the **settings** option.
+ Scroll down through the options to **parental controls.**
+ You'll be asked to **create a PIN.**
+ Enter a **4-digit PIN** and select **save**.

How to set up purchase restrictions

+ On the same parental controls page as above, select **purchase restrictions.**
+ Activate the **PIN on purchase** by selecting **yes**.

How to set up viewing restrictions and selecting certain devices

+ To enable content restrictions, select **viewing restrictions**, adjust the slider to highlight in green the specific age categories that **will NOT require a PIN** to access.
+ Press **save** to update your settings.

There are a number of options here :

U Universal Content Under 12 years
PG Parental Guidance /Over 12 years some content may not be suitable for under 12
15 Over 15 years
18 Over 18 years

Please note that you can select which connected devices will have viewing restrictions applied to them.

Apple TV

Apple TV is Apple's nod to smart technology. It's a handy streaming device you can plug into your TV. And with so many companies starting their own streaming services, Apple was never going to be far behind. Now they have Apple TV+ which you can subscribe to if you want to access any of their original programming. As with their other devices, the Apple TV comes with a suite of restrictions.

Restrictions available:
+ Inappropriate content
+ In-app purchases
+ Streaming media
+ Parental control

There's a wealth of options you can change, so let's run down our recommendations.

Setting up parental control restrictions
+ Select the **settings** app from the Apple TV home screen.
+ Then choose **general**.
+ From here, select **restrictions**.
+ Now select **restrictions** once more.
+ You will be prompted to enter a **4-digit passcode** if you don't have one created already. Re-enter the **passcode** to confirm it.
+ Finally, select **OK** to complete the set up.

Getting to the restrictions
Many of the next recommendations work from the same menu. So we're going to guide you to the **restrictions** menu, from which you can change all the relevant settings.
+ Select the **settings** app from the Apple TV home screen.
+ Then choose **general**.
+ From here, select **restrictions**.
+ Now select **restrictions** once more.
+ Enter your **passcode** when prompted.

There'll be a number of options available to you. Let's run through each one.

Restricting purchases and rentals
+ Select **purchase and rental.**
+ You can now choose what you wish to **restrict**.

Restricting in-app purchases
+ Select **in-app purchases.**
+ You can now **block** in-app purchases.

Restricting explicit music and podcasts
+ Select **music and podcasts.**
+ You can restrict explicit content by selecting the **clean** option.

Restricting music profiles
+ Select **music profiles.**
+ You can restrict music profiles by selecting the **clean** option.

Setting up content ratings based on a specific country
By default, Apple TV uses the United States ratings criteria for content. But you can easily change this to a country of your preference:
+ Select **ratings for.**
+ Choose the **country** of preference.

Restricting movies
+ Select **movies**.
+ Choose the **restriction** option.

Restricting TV shows
+ Select **TV shows.**
+ Choose the **restriction** you require.

Restricting apps

+ Select **apps**. You may have to scroll down a bit to see it.
+ Choose the **restriction** you want to apply.

Hiding explicit language in Siri

+ Select **'Siri explicit language'.**
+ Turn **on or off** as required.

Disabling multiplayer games

+ Scroll down and select **multiplayer games.**
+ Turn **on or off** as required.

How to disable screen recording in games

+ Scroll down and select **screen recording.**
+ Turn **on or off** as required.

How to restrict AirPlay settings

+ At the bottom of the menu, select **AirPlay**.
+ Turn **on or off** as required.

How to restrict conference room display settings

+ At the bottom of the menu, select **conference room display.**
+ Turn **on or off** as required.

How to restrict location services settings

+ Near the bottom of the menu, select **location services.**
+ Turn **on or off** as required.

How to restrict background app refresh settings

+ Near the bottom of the menu, select **background app refresh.**
+ Turn **on or off** as required.

How to restrict TV provider settings

+ At the bottom of the menu, select **TV provider.**
+ Turn **on or off** as required.

How to restrict remote app pairing settings

+ At the bottom of the menu, select **remote app pairing.**
+ Turn **on or off** as required.

BBC iPlayer

The BBC is the oldest British broadcasting company - it's literally their name. So it stands to reason they would also throw their hat into the streaming ring. You can watch and download the app on various devices, each with their own quirks.

Restrictions available:
+ Inappropriate content

BBC iPlayer has a wide range of content, so you want to ensure you enable the parental controls.

Setting up parental controls on your PC
+ Go to https://www.bbc.co.uk/iplayer
+ Select **parental guidance** at the bottom of the page or use this link https://www.bbc.co.uk/iplayer/guidance
+ Choose **lock now.**
+ Tick the **'I am aged 16 or over'** option.
+ Click **continue**.
+ Select **turn on PG lock.**
+ When prompted, create a **4-digit PIN.**
+ Click **save**.
+ The **4-digit PIN** will be required whenever someone tries to access age-restricted content.

Setting up parental controls on the smartphone or tablet app
+ Open the **iPlayer app.**
+ Select **menu.**
+ Then **settings.**
+ Next, choose **parental guidance.**
+ When prompted, create a **4-digit PIN.**
+ Select activate to save your **4-digit PIN.**
+ The **4-digit PIN** will be required whenever someone tries to access age-restricted content.

Setting up parental controls on the smart TV app
+ Open the iPlayer app on your TV.
+ Go to **settings.**
+ Then select **settings & help.**
+ Click **parental guidance** and start the setup.
+ Confirm you're aged 16 or over and create a **4-digit PIN.**
+ Select **OK** and confirm the **PIN**. Follow the rest of the instructions.
+ When the **'set up complete'** message appears, select close to return to the app.

eir TV

If you're in Ireland, you'll have access to something not everyone else will. eir TV is most closely related to something like Sky or Virgin TV here in the UK. It comes with its own app you can use to watch live TV and, as such, has a small range of parental controls.

Restrictions available:
Inappropriate content

This is only a short one and there's only one setting we recommend you change.

Setting up age restrictions

+ Select **parental control.**
+ Enter your **PIN** for the eir TV box which is provided on installation.
+ Select the appropriate **age rating.**

Netflix

Netflix is an incredibly popular streaming site. You could even say it kicked off the modern-day streaming boom. And with an almost endless array of content available - some child appropriate and plenty not - there's a lot your child will want to dig into. With such a wide range, it's important for children to have their own profile set up to restrict the content they have access to. All that's required is access to the primary Netflix account and the user password.

The primary account holder has two options for controlling access to content: they can set up a PIN or put a maturity level on a particular profile. So you have some flexibility in how you go about it.

Restrictions available:

+ Inappropriate content
+ Streaming media
+ Parental control

How do you set up these restrictions? Putting parental controls onto a profile is simple. Before we start, make sure to log into your profile on your PC as you cannot change this on the app.

Creating a child account

+ Select the option for **manage profiles**. There are a number of ways to access this:
    - » At the home screen where you select a profile, the option is underneath.
    - » On your personal page, you can select your profile picture in the top right and click **manage profiles.**
+ Click **add profile.**
+ Enter the **name** of your child (or use a fake one).
+ Next to this, there is a box that says 'child?' - tick this box.

Setting a PIN to restrict access

+ Select your **profile icon** in the top-right corner of the screen.
+ Next, select **account.**
+ Scroll down to **profile and parental controls.**
+ Choose which profile you want to change. We recommend adding a PIN to each profile, including yours, to prevent unauthorised viewing.
+ Select the option for **profile lock.**
+ When prompted, enter the password and click **continue.**
+ Here, you can create a **4-digit PIN**. This will be required to watch content or amend the settings.

Setting viewing restrictions on an account

+ Select your **profile icon** in the top-right corner of the screen.
+ Next, select **account**.
+ Scroll down to **profile and parental controls.**
+ Choose which profile you want to change.
+ When prompted, enter the password and click **continue**.
+ Here, you can change what age-rating the profile is allowed to watch up to. You can also block specific titles in the box below the age ratings.

NOW

NOW (previously Now TV) is Sky's online streaming service, offering TV shows, movies, and sports. It's an appealing system - there's no contract like their set-top boxes have. With so much content, we wouldn't be surprised if you're one of its many subscribers. But how does it compare to the rest of the market when it comes to parental controls? They are a bit limited, but available nonetheless there are things you can do to make it safer.

Restrictions available:

+ Inappropriate content restrictions

There's only one setting we suggest you change.

Setting up parental controls

+ On the nowtv.com homepage, sign into your account.
+ Select **my account.**
+ From the drop-down menu, select **parental controls.**
+ Follow the **onscreen instructions.**
+ If this is the first time on this page, you'll be asked to enter a **4-digit PIN.**
+ Now select the **appropriate age ratings**. By default, all will be allowed. But by changing them, it requires a PIN to watch anything over that age rating.

Samsung Smart TV

As a technology giant, we were bound to get back around to Samsung eventually. TVs are more their bread and butter, and they have a popular range of smart models. They have a limited range of built-in parental control features, so we recommend using them in tandem with the ones found on all your other services.

Restrictions available:

+ Apps access
+ Internet browser access
+ Inappropriate content
+ Streaming media

There are a few steps we recommend you take with your Samsung TV.

Setting a PIN

+ Bring up the **Eden** bar.
+ Scroll to the left and open up the **settings** menu.
+ Go down and select **general**.
+ Select **system manager**, then **change PIN.**
+ You will be prompted to enter your new **4-digit PIN** twice to set it and confirm it. If it asks you for an existing PIN and this is your first time, the default one is **0000**.

Changing your parental controls

+ Bring up the **Eden** bar.
+ Scroll to the left and open up the **settings** menu.
+ Go down and select **broadcasting**.
+ There are two options you'll want to change:
  - » Programme rating lock
  - » Channel lock

Setting up programme rating lock

+ Select the option for **programme rating lock.**
+ Enter your **PIN**.
+ Select the broadcasting rating as is required.
+ Once the broadcasting rate has been selected, only content suitable for the selected age will be available without the PIN.

Locking channels

+ Select the **apply channel lock** option.
+ Enter your **PIN**.
+ Select the channels you wish to lock.
+ Now, any locked channels will need to have the PIN entered to view them.
+ You can also delete channels, but you will have to re-tune your TV to find them again.

Locking apps

+ Bring up the **Eden** bar.
+ Scroll to the left and select **apps**.
+ The available apps will appear along the bottom of the screen. Select the ones you want to **lock**.
+ Click down on the menu with your remote and select lock.
+ Enter your **PIN** as requested.
+ There will now be a lock icon on the app - this means it needs a PIN to use.

Sky Q

Sky Q is like the 'deluxe' version of a Sky box. Designed for the modern age, it combines satellite television with catch-up TV and live recording. As you might expect of a 21st-century set-top box, it actually has some impressive parental control features. Of particular note is its 'kids safe mode' which temporarily locks away inappropriate content. As with many other services, this and other safety features will require a PIN. For Sky Q boxes, this will usually come on a card that comes with the box. We recommend you change this and keep the new one safe.

Restrictions available:
+ Internet browser access
+ Inappropriate content
+ Time limits

Let's take a look at what you can adjust on your Sky Q box.

How to change your PIN
+ Press the **home** button on your remote.
+ Scroll to **settings**.
+ Select **parental**.
+ Enter your current PIN to access the settings.
+ Scroll to **change PIN.**
+ Choose a **new PIN** that you'll remember.

Setting up kids safe mode
+ Press the **home** button on your remote.
+ Scroll to the **kids** section.
+ Choose the **safe mode** option.
+ Turn on the **kids safe mode** option. It will ask for your PIN.
+ Once you've done this, the Sky Q box will be locked and only kid's content will be accessible.
+ To turn it off, go back to the same section. You'll have to re-enter your PIN.

Enabling family settings
As well as kids safe mode, there's also a **family setting** which activates PIN-protected content.
+ Press the **home** button on your remote.
+ Scroll to **settings**.
+ Select **parental**.
+ Enter your current PIN to access the settings.
+ Go to **family**.
+ Turn on the option for **family setting.** This will put a blanket PIN protection on child-inappropriate content, including pre-watershed inappropriate content and on purchases. It can also hide adult content.

Restricting content based on age ratings
+ Press the **home** button on your remote.
+ Scroll to **settings**.
+ Select **parental**.
+ Enter your current PIN to access the settings.
+ Scroll to **ratings**.
+ Here, you can choose the age ratings that will require the PIN to access.

Restricting apps and videos
+ Press the **home** button on your remote.
+ Scroll to **settings**.
+ Select **parental**.
+ Enter your current PIN to access the settings.
+ Scroll to **apps & videos.**
+ Here, you can block access to online videos and various apps.

Sky Go

While similar to NOW, Sky Go is distinctly different. Sky Go is available to all existing Sky customers, allowing them to access everything they would be able to on their set-top box, but from a smartphone or tablet. To change any of its parental controls, you will need a Sky ID, which you can set up online. All you need is a contact email address and your Sky account number (if not those, then your direct debit details).

Restrictions available:

+ Inappropriate content

This is only a small section with one change to make.

Setting up content restrictions

+ Go to **go.sky.com** on your internet browser.
+ If you don't have a Sky account, select **sign up** and follow the onscreen instructions.
+ If you do have a Sky account, select **my Sky** from the menu at the top.
+ Now select **Sky Go PIN.**
+ You'll see options for the **access level** you can set on all of your Sky Go devices.
+ Once you select a level, you'll be prompted to create a **4-digit PIN.**
+ When accessing content on Sky Go, the **PIN** will be required if attempting to access the content you have chosen to restrict.

Virgin Media

Along with Sky, Virgin Media is a leading TV provider. If you're not a satellite household, maybe you prefer Virgin Media's cable access service? If you do, you'll be glad to know it comes with a whole host of settings you can change to ensure your child stays as safe as possible.

Restrictions available:
+ Inappropriate content

There's a nice selection of options available to you, so let's run through what to change.

How to set up a parental control PIN
+ On the remote, press the **menu** button.
+ Then select the **settings PIN parental controls** option.
+ Next, choose **PIN management.**
+ Then the **change master PIN code** option.
+ The default PIN is 0000.
+ Enter a PIN you will remember.
+ When prompted, confirm the PIN by entering it again.

How to restrict content by age rating
+ On the remote, press the **menu** button.
+ Then select the **settings PIN parental controls** option.
+ Next, choose **lock programmes by age rating** option.
+ Enter your **PIN**.
+ A list of age rating options will appear on the screen.
+ Select an age rating that is suitable for your children and select **OK**.
+ To view any content with an age rating higher than the one you have set, the PIN will be required.

How to lock specific channels
+ On the remote, press the **menu** button.
+ Then select the **settings PIN parental controls** option.
+ Select the **lock/unlock channels** option.
+ You can now go through the list of channels and choose which ones to lock.
+ The **PIN** will be required to access any of the channels you choose.

How to change the PIN using the Virgin TV Anywhere online player
+ Using an internet browser, open https://www.virginmedia.com/sign-in
+ Log in using your My Virgin Media **username** and **password**.
+ Select the **settings** option on the left of the page.
+ Then select the **parental controls** option at the top of the page.
+ You can now change the **PIN** within the online player.

How to change the PIN using the Virgin TV Anywhere app
+ Open the **Virgin TV Anywhere** app on a smartphone or tablet.
+ Log in using your My Virgin Media **username** and **password**.
+ Select the **settings** option.
+ Enter your **password**.
+ You can now change the **PIN** from within the app.

Some advice to parents about online sexual predators

If a child sexual predator came up with a platform where they could obscure their identity, get unlimited access to children, gather limitless information about a targeted child, without a fear of being caught, it would be the internet. This is a very heavy subject, one that no parent wants to think about, but it's the unfortunate reality of our world. And, as such, it's something we need to discuss. Some of these harsh truths may be distressing, but we need to hammer home the point of just how simple it is to access children and how this can have long-term damaging effects.

Online sexual predators, regardless of whether they are contact or non-contact offenders, currently have unrestricted access to an entire planet full of innocent children. They have an all-too-easy way to develop a trusting relationship that can gradually be strengthened over time. By sharing images, they can slowly desensitise a child by introducing them to pornographic concepts and content. They can gather information about a parent's involvement in the child's online life, allowing them to weigh up the chances of being caught and how far they can push their luck.

It has never been easier to get access to vulnerable children of all ages. Neither has there been so many victims of child sexual abuse all through a single medium. And, if you look in the right dark corners, you'll find communities where sexual predators can collaborate.

A way to educate each other in the best techniques to entrap children. It offers a way to hunt in packs to target children - a live 24/7 market place to trade and traffic the images and videos of the horrific sexual abuse of children. They surround themselves with so many like-minded people that their behaviour becomes validated, justified, and normalised.

According to former Homeland Security agent Tim Ballard, the trade in the sexual abuse and trafficking of children is valued in the region of $150 billion a year. The illicit business has become more profitable than the global weapons trade. It's due to surpass and become more profitable than the global drug trade in the next few years. At present, there are approximately over 9 million child sex slaves out there right now. This dark and disgusting world exists right under our noses. Given how prevalent the online sexual abuse of children is, you might think the authorities are getting the upper hand. Unfortunately, globally, they are not. Every second, another child becomes a victim. Often in their own homes, with their parents only a few feet away from them.

What terrifies us most when we talk with parents is the mistaken belief that their children are safe at home. People tend to focus more on the obvious dangers outside the home, yet are blind to the reality of an online sexual predator getting digital access to a child. It's horrifying to imagine, blissfully unaware about what's happening in the next room. With 75% of all child pornography images being self-generated, we cannot put enough emphasis on how truly vulnerable children are online. Parental controls will assist you, but ultimately, they will not protect a child. Not if they have unrestricted or unmonitored access to the internet.

The most frequently asked question we get asked is which are the most dangerous apps. The simplest answer we can give is that no one platform is any safer or more dangerous than the other. It comes down to how the app operates, whether it's age appropriate, or whether the child can talk to other people. The primary concern should always be whether strangers are able to contact a child on the platform. Also, parents have to be mindful of whether a complete stranger can gather or harvest personal or private information. Information such as likes and dislikes are often used to build up an affinity with a child. This is the first step on the road to sexually exploiting a child online.

What makes it so difficult is how easily online sexual predators can obscure their real identity. Very often, they'll spend a huge amount of time creating hundreds of profiles across multiple platforms, sometimes posing as a young person themselves. There, they'll do something we mentioned before - they'll become 'lurkers'.

For online sexual predators, being able to mix in without suspicion is key to maximising their chances of success. The ability to go unnoticed while watching and observing young people allows them to build up that profile. Generally, they'll make little contribution themselves, preferring to stay silent. They do just enough to make the profile seem legitimate and convince others the account is genuine, and has existed more than just a few days or weeks. This gives an online sexual predator greater opportunity to engage with others and become part of online communities. People tend to like people who are similar to them. By observing the posts and comments posted by a targeted child, they can build up a rapport by pretending to have similar interests.

Online predators will get to know and understand their victims, waiting for the right moment to make their move. This is where a child who has been educated to look out for the signs of an online sexual predator can immediately stop the interaction with this "stranger". Unfortunately, the number of children who will take the step to block, report, and tell parents are currently nowhere as high as we need them to be. Sadly, children do engage. It might just start with a simple compliment. We can't help but feel happy when someone (seemingly genuinely) compliments us, and this can be enough to make a child drop their guard.

Gauging the level of interaction, the online sexual predator will now know whether it's appropriate or not to increase the level of contact. For a child who's socially isolated at home or school, the engagement of a total stranger who claims to also have similar interests and experiences can be enough for a connection to be made. Being attentive to the needs, wants, and emotions of a child are key to luring them into an environment where they believe this is a person who understands them. The more compliments, support, and encouragement the child receives, the greater the chance they will disclose more about themselves. By sharing similar thoughts

and emotions, the online sexual predator can offer their own very personal self-disclosures, which will ultimately lead to an exchange of secrets. Secrets are exceptionally powerful as they afford a huge level of trust and give a level of control, especially if it's something they would rather not have anyone else know. That false vulnerability encourages the child to do the same with their very real secrets, giving the predator a tool to blackmail with - if they so wish.

The simplest attribute needed to be a successful online predator is having the ability to listen. Listen to those who want to be heard. Listen to the millions of children who are now more socially isolated from each other than ever before. They act as an active audience that's always willing to pay attention to them. To a child who just wants some attention, connection, or friendship, it might be all they need.

Relationships develop very quickly online for both adults and children. Known as the hyperpersonal model, this is the idea that we come to like each other much quicker when not face-to-face. Despite seeming so impersonal, online communication is often perceived as more personal than usual. People have a greater ability to change how others perceive them, optimising traits or characteristics that they may lack in the real world. Because there's no body language, we put more stock in the words used. This, combined with the anonymity, allows online sexual predators to thrive. In short, this leads to an online relationship developing with a deeper sense of intensity and far more quickly than it would in reality.

Children from broken homes or dysfunctional families are often thought of as being the most at risk. But with families becoming far more distant thanks to technology, it's not always the case anymore. Captured by the all-consuming glow of a screen themselves, children as young as five and six will openly speak about how their parents overuse technology. These are the children who are now equally at risk. Children who crave the attention of a parent who always appears distant or hasn't got the time to spend with them. Parents need to be aware that, if you don't give the attention that children need to develop, they will ultimately seek it out online. Unfortunately, that might lead them to particularly unsavoury characters.

It doesn't help that children often believe they know how to handle unwanted contact by themselves, without ever discussing it with parents. We've heard of a multitude of strategies they've developed over time. Essentially, they all involve some form of lying about their name, age, or where they're from. For the most part, this is initially unimportant to many online sexual predators. What they're interested in is how a child will react. Even if the child blocks the new contact, the damage has already been done. Online predators will use their multitude of other profiles to try to get the child to open up a bit more. Once they do, the grooming process commences.

A 2017 Swansea University study found that it can take as little as twenty minutes to groom a child online from the moment of first contact. That's literally in the blink of an eye. A parent goes to prepare their child's dinner, and by the time it's ready, they could already have exchanged sexualized images of themselves with an online predator. Time is an important factor in helping to protect children online. The longer they're left exposed to an unmonitored and unrestricted online world, the greater the chance of them experiencing something harmful. The times at which the child uses digital devices and where in the home they're allowed to use them really need to be given some thought.

No child should ever be able to access the online world in their bedroom. We'd go as far as saying they should never go into the bathroom with a digital device either. Much of the generated content by children is made from both their own bedroom and in the bathroom of the family home. Live streaming has opened the door for online sexual predators to sexually exploit and abuse children on a whole new level. Once they have control over a child, they can force them to take more and more videos and photos on demand. And it might not come from just one predator; there may be several. Children feel exceptionally trapped in these situations. Very few will ever even recount their experiences to anyone. Those who do require an enormous amount of help and support for many years after to recover from their life-altering experiences.

This threat is very real. Complacency leaves them an open target. The proliferation and normalisation of this issue has reached unparalleled proportions. Children as young as eight and nine have told us they've been asked for unsolicited sexual images.

Above and beyond children living as sex slaves,

there's even been a push by the paedophile community to rebrand themselves as a socially accepted sexual minority, tryting to worm their way into the LGBTQ community as MAP - "Minor Attracted Persons". While such emboldened and public people will be few and far between, we can never underestimate how trends develop and where they may go. We will never see them accepted by society at large, but the fact they are willing to be so open about it makes you wonder where they would stop.

What has given us serious and exceptional pause for thought in recent years is the ease at which paedophiles were getting access to children online. Thanks to the likes of Mick Moran - assistant director of the Vulnerable Communities Sub-Directorate at Interpol - and James Neary - who has been decorated by the FBI - the fight for the safety of child victims continues.

We all need to support the hard working and selfless individuals that go to work every day and see the unimaginable. Those who will carry the pain and suffering of the victims who are being sexually abused for life. We need to get on board with them and do everything possible to prevent a child becoming a victim. To report and respond to every cry for help. We need a community - the online community - to be forthright and honest in making every attempt to protect children online.

Yet we continue to have difficulty in getting parents to listen to this message. Parents who are too busy, those who believe they've heard it all before, and never turn up at school presentations. While cyberbullying is an important issue for us, the online sexual abuse and exploitation of children has always been our core message. Very often, the most vulnerable children we meet - the children who have ridiculous access to the online world - are never represented by their parents.

This active threat to children is very real. Ignore it at your peril. As we've said in the past, parents are on the front line. If children have access to the internet, online sexual predators have access to them.

It's estimated that one in every four children are victims of child sexual abuse. That's a considerable amount of children. Unfortunately, on average, it takes up to 22 years for a victim of child sexual abuse to come forward. We need to ensure we do everything possible to protect children from being exposed to a paedophile in the real or online world. Make no mistake, online sexual predators will have taken advantage of the COVID-19 pandemic. We know there's been an explosion in the number of children targeted online. How bad of an attack will only be identified in time to come.

"Children are genuinely at serious risk of harm online if we can't get parents on board with us."

Children are genuinely at serious risk of harm online if we can't get parents on board with us. They can't be expected to have the ability to deal with this danger alone. Parents are the ones with the means and methods to protect their children. But they have to consciously decide to make an effort. Not a half-hearted attempt. Parents need to be vigilant and fully cognisant that there's a very high chance that an online sexual predator will at some point make contact with their child. In fact, there is every likelihood that multiple online sexual predators will make contact with them. Unless you're part of your child's online life and have ensured every precaution, then they're at risk.

Even simple changes with regard to device access in the home can make an enormous difference. Ensure that your children only use digital devices in a room downstairs where you can keep an eye on them. Under no circumstances should they be permitted to use the technology in their bedroom or bathroom. Devices should all be kept together at a central charge point downstairs at night. No devices should ever be permitted in a bedroom overnight. Finally, ensure that the Wi-Fi connection is switched off at night and mobile devices are either locked away or have software downloaded to manage screen time. This is a gateway that should be secured and closed just like the windows and doors of the family home.

7

Internet browsers and search engines

As a parent, you never stop worrying about your child. There are already so many factors you need to be mindful of in the real world without having the extra burden of thinking about what's online. Not everyone can be expected to manage all of these threats all of the time. Eventually, something gives - usually your attention that's drawn elsewhere. No parent can be omnipresent, so you shouldn't ever feel like you're expected to be. However, when we neglect a child's safety online, due to the overload of everything else, the consequences can be tragic for either the child, the family, or both.

A parent's job is tougher than ever, trying to juggle all of the real-world responsibilities on top of attempting to absorb all this extra information regarding technology, apps, consoles, games, and more. Parents now also face an additional threat of compromised digital devices and the family's online life and accounts. The risks of financial harm are high and effortless: a single click on a link could open a malicious website and lead to a nightmare scenario.

There are multiple ways to infect digital devices. Malware is the generic term used to describe software that is "specifically designed to disrupt, damage, or gain unauthorised access to a computer system". And it comes in many forms. Most people are familiar with computer viruses, but there are also other forms of malware, such as a Trojan virus, worms, ransomware, spyware, and adware.

Many of them use social engineering to make their way onto your devices. These are basically designed to take advantage of the natural human tendency to trust. This type of attack works successfully due to the way it manipulates people's emotions, especially the negative ones. When you're put under stress and have to make a hurried decision, there's a high likelihood that you'll make a mistake. They also take advantage of our own perceptions of the world, such as how we view an authority figure. People are far more likely to fall for one of these scams if they believe the person or company responsible are to be trusted. You may be familiar with fake emails purporting to be from Apple, suggesting you click on a link and sign in to your account to confirm purchases you never even made.

There's a large variety of social engineering attacks. Some of the more common include phishing, spear phishing, whaling attacks, vishing attacks, pretexting, baiting, tailgating, quid pro quo, and what's known as a watering hole. The purpose of listing these is to show you how vast this area is. Children don't stand a chance against these attacks due to their impulsive nature. When children see a piece of adware that says "get your FREE VBucks for Fortnite by clicking here", that's your device well and truly compromised.

"Children don't stand a chance against these attacks."

And that's not an exaggeration; we've heard plenty of stories from parents whose children gave away their personal information so they could get their free loot boxes or skins for whatever popular game they were playing. Scams like these only work because kids don't realise there are unsavoury sorts on the internet. A couple of days later, there's a problem with the device or - in the worst-case scenarios - bank accounts. And your child will still never get their skin or VBucks.

From an early age, we have to teach children that if something seems too good to be true, it usually is. They need to understand there's no such thing as "free" when it comes to the online world. Generally, anything that's free has a personal, financial, or other cost attached, you just might not be able to immediately see it. Children should never sign up for or download anything without your full knowledge and approval. It's incredible just how many kids we've met who have complete free reign over all of the digital devices in the home. The parents were often completely unaware of the many various attacks that target children specifically.

To protect your information, every device should have an antivirus installed. There are a wide variety available, ranging from free solutions to reasonably priced software you can put on any device in your home. We would recommend using a paid service as these often have more features you can use. You also need to consider using a VPN (a 'Virtual Private Network') especially if you use devices in the outside world. These mask your real location and allow you to browse the internet in privacy.

We usually tell parents to make sure their children don't have access to a device with administrator privileges. This means no private files, documents, or personal and financial information on the device. Children will make mistakes. When they do, you want to be sure you aren't at risk.

Good online hygiene is essential to protect the family as a whole. Teach children to always check with you first if they have any doubt or concern. We want them to avoid clicking on or downloading content while you're blissfully unaware of what's at danger. You won't realise until days, weeks, or months later when you notice your money has suddenly disappeared.

Children are far less experienced than adults. They're also far more trusting than adults. A deep level of distrust is needed when navigating the online world. That isn't built up overnight. It's something that's learned over time and only by you teaching your kids how to spot potential hazards and risks. They have to learn the importance of not sharing their personal information with anybody. People, messages, emails, and websites can appear very authentic now, so it's a steep learning curve for adults to learn about the methods being used to exploit people.

Keylogger
A keylogger is a simple piece of software that records what you type on your keyboard. It saves this information and forwards it to whoever created the exploit. This can affect a PC, tablet, or smartphone. With this information, they can log into any accounts you used while the keylogger was active. You might not even be aware that your device has been infected.

"The number of these attacks is increasing year on year."

Denial of Service (DoS\DDoS)
A "Denial of Service" attack, or a "Distributed Denial of Service" attack, is used to take down a website or a server by overwhelming it with a huge amount of traffic. Since it can't deal with all of these attempts to access it, it ends up crashing and going offline. The number of these attacks is increasing year on year.

Watering hole attacks
Have you ever seen a free Wi-Fi network while out in public? It may just be a "watering hole". Just like in nature, they're set up as a public area for users to congregate, unaware that someone is waiting for them. It looks like an authentic connection, but someone will be capturing the internet traffic. And because it's free, it's too tempting for some to not use. We would recommend you stay away from "free" networks - like we've said before, there's always a cost. If you have to use them, it's good practice to have a VPN to encrypt your data.

Passive attacks
When you use a network, your device communicates with it by sending small packets of data. But if these aren't protected by a VPN, they can be captured by third parties with little effort. There are also variants that will sit on the device and monitor all activity, without you ever knowing. The software will not harm or damage the device, it will simply sit and watch. This may include all activity both on- and offline. At its most insidious, it may also be able to activate the microphone or camera.

Phishing
A phishing attack is when someone tries to deceive you by pretending to be a reputable business. You may have seen one yourself; a popular one is someone pretending to be from your mobile network provider saying you have an outstanding bill. It usually comes with a suspicious link that, when clicked, will take you to their website where they will either harvest your financial details or simply install some malware. Never click on any link you receive in an email or message unless you're absolutely sure where it's come from. By right clicking on a link (or holding down on a mobile), you can see the web address. Very often, this is a dead giveaway - it won't be the usual one the company uses. Bad spelling and grammar in the email may also be good indicators.

Viruses, Trojans, and worms
Viruses, Trojans, and worms are malicious software programs used to access a target's system and do something like install a keylogger or steal sensitive information. They can be also used to freeze or lock the target out of their device. They can spread to other devices if connected to the same network and through the contacts. These can also be used to turn a target's device into a zombie machine that will become part of a larger network to be used in DDoS attacks.

Clickjacking attacks
Clickjacking - also known as UI redress - is a very common tactic, especially for unknown-source app downloads, illegal movie streaming, and torrent websites. The link will look like one thing, with you expecting it to take you somewhere in particular, but it will take you somewhere completely different. While they're often just designed to earn money through clicking adverts, some do use them to steal personal information.

Bing

If you own a Microsoft device - such as a Windows PC - you'll probably have come across Bing. Microsoft's answer to Google, Bing is their proprietary search engine. Most people will change to Google, but if you're a fan of Bing - or have never thought to change your default search engine - then you'll want to know what you can do with it.

Restrictions available:

+ Inappropriate content

It doesn't have many options you'll want as a parent, but we at least recommend turning on safe search.

Setting up SafeSearch

+ Open up www.bing.com
+ Click on the **settings** tab at the top of the page.
+ From the drop-down menu, select the **settings** option.
+ Then select **more**.
+ In the SafeSearch section, set it to **strict**.
+ Click **save**.

Microsoft Edge

What Bing is to Google, Edge is to Chrome. If you use a Microsoft PC, Edge will likely be your default browser. It used to be known as Internet Explorer, but after a bit of rebranding and redesigning, Microsoft has created the very functional Edge. There are a few more options available to you as a parent, so used in tandem with Bing, you can create a relatively safe space for your children to browse the internet.

Restrictions available:

+ Inappropriate content

Here are the settings we recommend you change.

How to turn on the SmartScreen filter

The SmartScreen filter blocks and warns about sites that might be unsafe for the user.

+ Click on the **three dots** at the top-right corner of the screen in the Edge web browser.
+ Select **settings**.
+ Then **privacy and security.**
+ Scroll down to **security**.
+ Under the heading **Windows Defender SmartScreen**, switch the option to **on**.

How to block auto-playing audio or video

+ Click on the **three dots** at the top-right corner of the screen in the Edge web browser.
+ Select **settings**.
+ Then select the **advanced** option.
+ Under **media autoplay,** open the drop-down menu of **'control if audio and video play automatically on sites'.**
+ Select **block**.

Google

The ultimate search engine. Google's hold on the market is incredibly dominant, with over 90% of people using it for their browsing needs. We'll get to Google Chrome in a moment, but let's start with the search engine - specifically its SafeSearch option. SafeSearch is a very handy tool for parents which can help you block inappropriate or explicit content from search results. While no content filter is 100% accurate, it's certainly better than not having one at all. There are two options available: either having the safe search enabled for single session use or, what we would recommend, having it activated for all searches.

Restrictions available:

+ Inappropriate content

Here's how you can turn SafeSearch on.

Activating SafeSearch

+ Go to the homepage at www.google.co.uk
+ Go to **search settings.**
+ Under **SafeSearch filters,** tick the box next to **turn on SafeSearch.**
+ Select **save**.

Change your child's SafeSearch settings in the Family Link app

For Google account users under 13, or for Google accounts managed with Family Link, SafeSearch is on by default. If you followed our steps earlier to set up Family Link, you won't have to do anything at this point. Should you want to turn it off for whatever reason, you can follow the steps above.

Google Chrome

Unlike with its search engine, Google's share of the browser market isn't quite so dominant. Don't get us wrong, they still have over 60%, but Safari (often accessed on Apple products) and Firefox offer a bit of competition. But since they're the market leader, you would hope Google had made some consideration into their safety and privacy features. Thankfully, they have! Google Chrome offers a number of parental controls. However, these only work with Google Family Link. The Chromebook affords similar - again Family Link is important. Children need to be signed into their own account to benefit from the parental controls available.

Restrictions available:

+ Inappropriate content
+ Content restriction
+ Content supervision
+ App restrictions

Let's start with supervised accounts. As we mentioned, these won't work without Google Family Link, so when you've proceeded with these steps, make sure to download the app.

Adding a new supervised account

+ Sign into Chrome and select your **profile picture** in the upper-right corner of the screen.
+ Select **add another account** from the menu.
+ Enter the child's details and choose a profile picture.
+ The select **add person.**
+ When prompted, turn sync on. This is a very important feature as it allows you to see the account activity, including the history, passwords, and other settings. Any changes to the account will automatically sync to the parent account.

Adding a new supervised account on a Chromebook

+ Sign into your account on Chromebook.
+ Click on your **profile image** in the lower right-hand corner of the screen.
+ Select the **settings** icon.
+ Scroll down to people then select **manage other users.**
+ Under users, select **enable supervised users.**
+ Select **done** to save the setting and return to the previous screen.
+ Click your account photo at the bottom right-hand corner of the screen, then **sign out.**
+ On the Chromebook's login screen, select more at the bottom of the screen, represented by **three vertically-aligned dots.**
+ Then select **add supervised user.**
+ Read the information displayed then select **create supervised user.**
+ You'll now need to select the **profile** which will be the managing account and then enter the password when prompted.
+ Select **next** to continue.
+ Choose a name and password for the supervised user profile image and select **next**.
+ The supervised user profile has now been created.
+ Once the set-up is complete, a confirmation page will appear on the screen.
+ A confirmation email with more information will also be forwarded.
+ Finally, select **got it** to return to the login screen.

Blocking or approving access to websites

+ Open the **Family Link** app.
+ Select the **account** in question.
+ Go to **settings**.
+ Click **manage settings**, then **filters on Google Chrome,** and finally **manage sites.**
+ Choose which category you want to edit - the **approved list** or **blocked list.**
+ Change as appropriate.

Get notifications if restricted content is accessed

+ Under **manage user,** select **notifications are off.** Notifications are set to off by default.
+ Select **turn on.**
+ If your child tries to access a blocked site, you'll receive a notification.

Turn off autofill passwords

+ Go to **settings**.
+ Select **autofill**.
+ Select **passwords**.
+ Under **offer to save passwords**, set the button to **off**.

Blocking inappropriate images

+ Go to **settings**.
+ Select **advanced settings.**
+ Click **privacy and security.**
+ Choose the option for **site settings.**
+ Select the **images** option.
+ Turn off the **show all** options.
+ You can also now manually allow or block websites from showing images.

Chrome parental control extensions

Google Chrome allows you to add extensions that improve its functionality. There are plenty of ones designed for parents, and here's what we highly recommend:

Blocksi

This is an all-in-one parental control extension. It allows you to enforce time restrictions on a number of categories, so you can ensure when they go to bed, they've really gone to bed! You'll also have the option to block specific online content, view web history, analyse trends of your child's internet browsing activity, and get warned when blocked content is accessed.
https://blocksi.net/

WardWiz iOS Essentials, Android Essentials, and Essentials Plus

This parental control suite by WardWiz provides complete cyber security and a range of options, such as blocking keyword searches, locking the App Store, and managing screen time.

You can also set a geofence around the child's location (such as the cinema or a friend's house); if your child leaves that zone, you'll know about it.

Opera

While not the most popular browser around, Opera is a nice little browser that you can't go wrong with. It's main selling point is its focus on safety and privacy, with a free VPN built-in. While free VPNs are an option, you tend to get a better service from a paid solution. But if you don't want that extra cost, Opera might be the way to go. As for parental controls, it has a few settings available.

Restrictions available:

+ Inappropriate content

There are a couple of suggestions we recommend if you do choose to install Opera.

How to block images

+ Go to www.opera.com
+ On the home page, select the **main menu.**
+ If you can't see the settings icon, click on the **three dots** at the bottom-left corner then click **settings.**
+ Select **advanced**.
+ Then choose **privacy and security.**
+ Select **site settings**.
+ Next, choose **images**.
+ Make sure the **show all (recommended)** option is in the **off** position.
+ You can also now block websites from displaying images by entering the site URL under the **block** option.

Turn off autofill passwords

+ Go to www.opera.com
+ On the home page, select the **main menu.**
+ If you can't see the settings icon, click on the **three dots** at the bottom-left corner then click **settings.**
+ Select **advanced**.
+ Scroll to the **autofill** section.
+ Select **passwords**.
+ Uncheck the **offer to save passwords** option.

8

Windows operating systems

Windows 10

Do you remember Windows 95 like us? Our apologies if we're making you feel old! But as much as we'd like to stick with what we know, it's much safer staying current with the operating system. Windows 10 is the most recent one, and we recommend you upgrade if you haven't already. It's going to be the one that receives the most updates, ensuring it's always as safe as possible. And most software is going to support Windows 10. If you've bought a new computer, it will likely have this pre-installed.

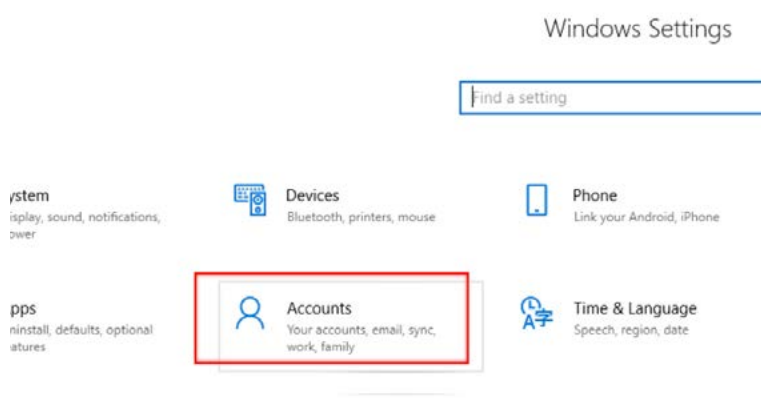
Restrictions available:

+ Inappropriate content
+ Monitoring
+ Supervising
+ Spending
+ Time limits

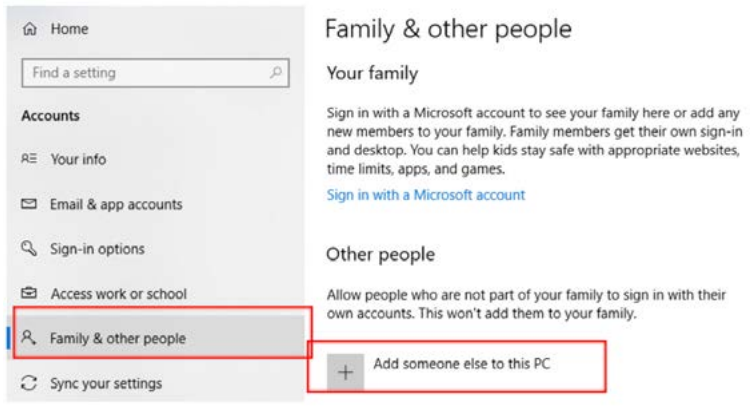
As a parent, there are a lot of changes you can make to keep your children away from inappropriate content.

Setting up parental controls

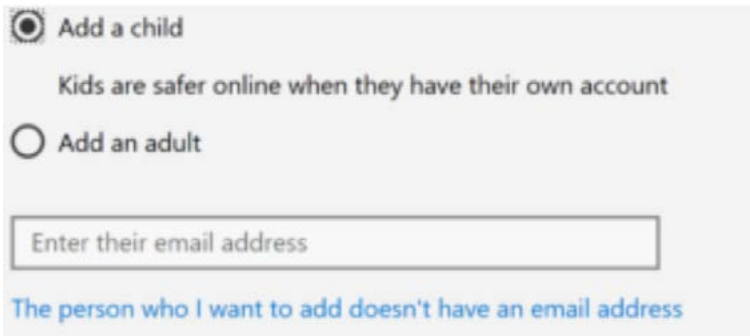
+ Log into the **administrator account** (or an account with admin rights).
+ From the desktop, click on the Windows icon in the bottom left of the screen.
+ Select **settings** (the cog icon) to open the menu.
+ Click on the **accounts** option.



+ Select the **family & other people** option.
+ Then select **add someone else to this PC.**



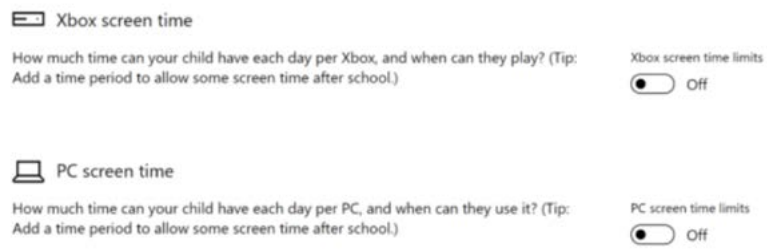
+ **Add a child** then enter your child's Microsoft email address and select **next**.



+ Enter your mobile phone number.
+ Untick both boxes on the next screen.
+ Read the message and ensure you write down the **account.microsoft.com/family** web address. This will be used to monitor and alter your child's account.
+ Select close once you're ready to continue.
+ You'll now see the newly created account under your family. Your child can now log into their own account on this computer.
+ To ensure your child is fully protected, they must be **logged into their account** when using the computer.

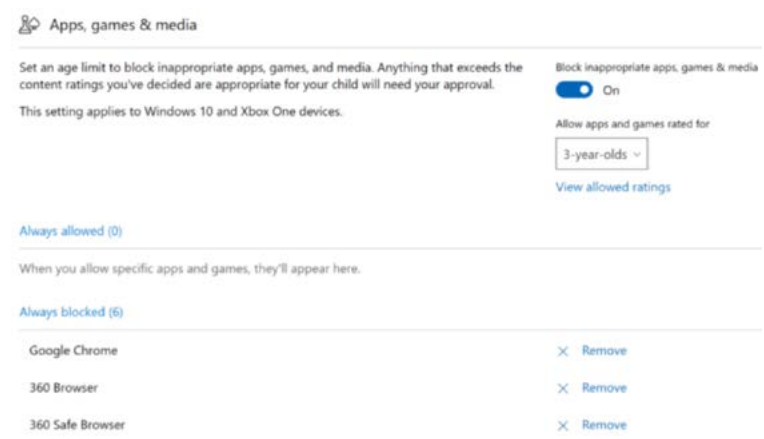
Changing screen time

+ Select the **screen time** option.
+ You can see the screen time details for each device your child is logged into. You can now set time limits on these devices by activating the **screen time limits** option.



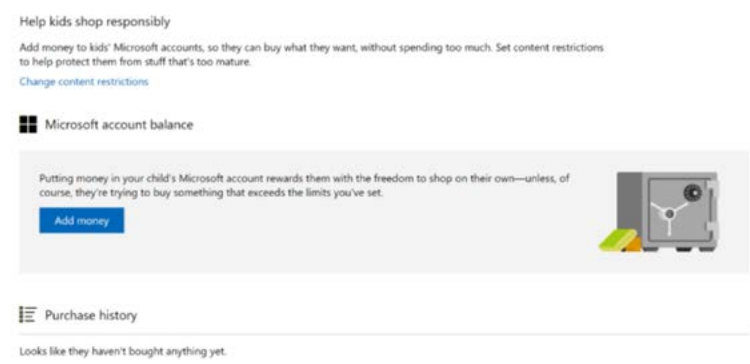
Restricting content

+ Select the **content restrictions** option.
+ This option allows you to set purchase limits, age limits for games and apps, block applications, and block websites or set a list of websites that are accessible. The web restrictions only work on Edge, so ensure other browsers are blocked.



Limiting spending

+ Select the **spending** option.
+ Here you can decide if your child is allowed to purchase anything from the Microsoft Store. You can also view their purchase history.



Windows 8 and 8.1

Windows 8 was released in 2012 to mixed reviews. It was the first edition to embrace tablets, and the OS was designed to work on both mobile devices and PCs. Windows 8.1 was a mix of Windows 8 and more traditional PC features and was generally more popular. Both Windows 8 and 8.1 haven't been supported for quite some time, meaning they aren't receiving the most up-to-date security features. So doing what you can to keep users safe is of the utmost importance.

Restrictions available:

+ Monitoring
+ Restrictions
+ Inappropriate content
+ Time limits

To enable parental controls in Windows 8 and 8.1, you first need to create an account for your child.

Creating a child account

+ From the keyboard, hold down the **Windows key** and press **C.**
+ Click **change PC settings.**
+ Select **accounts**.
+ Next, choose the **other accounts** option.
+ Then click **add an account.**
+ Select **add a child's account.**
+ Follow the prompts to complete the process, opting to create a Microsoft account over a local account if possible.

Setting up parental controls

+ Open the **Control Panel**. You can search for it from the Start screen or from the desktop.
+ Click **user accounts and family safety,** then choose **set up parental controls for any user.**
+ Choose the child's account.
+ Under **parental controls,** click **enforce current settings.**
+ Next, go to **activity reporting**.
+ Select **collect information about PC usage.**
+ Click the links provided for the following options and configure as desired:
    a. **Web filtering** to block certain websites and prevent downloads.
    b. **Time limits** to choose when and on what days your child can access the PC.
    c. **Windows Store and game restrictions** to set age, title, and rating limits on the apps your child can use.
    d. **App restrictions** to set the apps that your child can use.
+ You'll receive an email that includes information about the Microsoft Family Safety login page and what's available there. If you use a Microsoft account for your child, you'll be able to view activity reports and make changes online from any computer.

Windows 7

Windows 7 was an incredibly popular OS, so we wouldn't blame you if you still had a PC that was running it. As of 2020, it's no longer supported by Microsoft, making it vulnerable to people exploiting its insecurities. While we highly recommend upgrading to Windows 10, it does still come with some nice tools for you to use.

Restrictions available:

+ Block programs
+ Time limits
+ Inappropriate content
+ Content restrictions
+ Parental monitoring

You can configure parental controls in Windows 7 from the Control Panel, in a similar manner to what's outlined above for Windows 8 and 8.1.

Creating a child account

+ Press the Start button in the bottom left of the screen and open the **Control Panel.**
+ Then select **user accounts.**
+ Next, choose the option for **'give other users access to this computer'.**
+ Now work through the process as prompted on screen.

Enabling parental controls

+ Click the Start button and type **parental controls** in the search window.
+ Open **parental controls** from the results.
+ Select the child account.
+ If prompted, create passwords for any administrator accounts.
+ Under parental controls, select **enforce current settings.**
+ Click the following links and configure settings as applicable: **time limits, games, and allow and block specific programs.**

9

Gaming consoles

There has been an absolute explosion in gaming. The infamous massive multiplayer Fortnite is by far one of the most popular games of all time, and one that's a favourite among all of the children we meet. Fortnite player Kyle Giersdorf, AKA Bugha, was only 16 when he earned an almost unbelievable $3 million after winning the Fortnite World Cup in July 2019. And that's just a small slice of the incredible $30 million in total prize money that was handed out during the Fortnite World Cup. Even this was only part of the $100 million prize pot given to players in 2019. It can be mind-boggling to contemplate how such vast sums of money can be given away for a video game.

"The whole dynamic of gaming has changed over the last few years."

But when it brings in literal billions for Epic Games - Fortnite's creators - it makes a lot more sense. With over 250 million players worldwide, each player spending on average up to $85 each on in-game purchases, it's easy to see how the Fortnite business plan was such a huge success. And you can see why children want some of that glory people like Bugha get.

The whole dynamic of gaming has changed over the last few years. It's moved far beyond a solitary activity to being a very social one. Gamers can now play with family, friends, and strangers from all over the world. The social aspect of gaming is an important part of its success. However, parents do have justifiable fears regarding online gaming. Internet Gaming Disorder is now recognised and acknowledged by the World Health Organisation. Gaming has been found to be a source of serious addiction for some, both young and old, around the world. Some of the more extreme examples of excessive gaming originate from Asian countries, where young males have essentially died from deep vein thrombosis whilst sitting playing online games for days on end at a time.

Parents also need to be mindful of the potential harm excessive gaming can do to a child's development, not to mention their academic performance. We've seen plenty of children who stay up until the early hours of the morning, wreaking havoc on their sleep patterns. Humans don't do particularly well if sleep deprived; you become more susceptible to illnesses, are exceptionally prone to errors in judgement, and struggle to concentrate. From our perspective, as people who have delivered presentations to children and teens, it's incredibly easy to spot the ones who are present in body but not in mind. You can see the dark circles under their eyes. Teachers are sometimes amazed at how easy it is for us to identify kids who are clearly showing signs of excessive technology use.

Gaming can lead to children isolating themselves completely in a virtual world. Left unchecked over time, this may have a detrimental impact on their ability to engage with others in the real world. Social skills are an essential aspect of how we communicate with one another. Any child lacking in this area may develop social anxiety, which can be very debilitating the older you get, especially in the teenage years. Children also tend to reduce social interaction in the real world to only those who they're interacting with online. Unless it's addressed, the problem only gets worse as the child gets older. Trying to bring a child back to the real world can be quite difficult and distressing for both the child and their parents.

"We also need to be mindful of the ever-constant risk of online sexual predators praying on children who play on more popular gaming platforms."

Then there's the content of the games themselves. Some of the most popular ones are highly inappropriate for children, such as Grand Theft Auto 5. The Call of Duty series is all about bloody and brutal wars. One game that failed to launch in 2019 was Rape Day. The name alone should tell you why there was an uproar among parents.

We also need to be mindful of the ever-constant risk of online sexual predators praying on children who play on more popular gaming platforms. As we said in an earlier chapter, they often pose as children themselves. They try to befriend kids by offering help, resources, weapons, or in-game currency, all in the hope of gaining trust and friendship. Once they have that, they try to encourage children to move onto more discreet platforms for private communication with the ultimate aim of sexually exploiting or physically sexually abusing the child.

If all of this negativity wasn't enough, parents also have to contend with in-app purchases and loot boxes which feature heavily in almost all games now. This has been likened to gambling due to the similarity with casino games. You're hooked on the idea that you're one pull away from a big win, just like a slot machine. If a child wants that one particular skin that looks cool, they'll spend as much money as they need to get it, not realising it's actual real-world money that's paying for it. It doesn't help that many games use their own form of currency you have to buy with actual money, obfuscating the value of it and blurring the lines between what's real and what isn't. This is on top of many other small yet insidious tactics they use to squeeze out as much from you as possible.

With all this in mind, where do you start? Begin with the games your child currently has access to. Are the games age-appropriate? Up until September 2019, we were seeing a frightening number of young children who had access to GTA5, which is about as adult as you can get. There's since been a mass migration to Fortnite and Apex Legends, which is at least a little better. Fortnite has a 12+ age rating, while Apex Legends is targeted at over-13s.

It's important for you to know the difference between an online game and an offline one that isn't connected to the internet. Some are designed to be wholly online experiences - such as Fortnite - while others are only offline - like a Pokemon or Mario game. Then there are those which can be both, such as Minecraft.

"It's when children access games outside their age range that issues can start to arise."

Today, there are plenty of games integrating online aspects. Players from all over the world join together to play the same game. Some of these, like the aforementioned Minecraft, have a lot of positive aspects to offer young players, from both a social and developmental point of view. It's when children access games outside their age range that issues can start to arise. Whatever game your child is playing, you need to know what it involves. This is a list of questions to ask yourself before you give your child access to any game. You can also apply these questions to the games downloaded from the Google Play Store or from the Apple App Store.

+ Is the game age-appropriate?
+ Are there parental controls?
+ How do players interact and communicate with each other?
+ Are there facilities to report and block problem players?
+ Can my child be cyberbullied in the game?
+ Can strangers access my child through this game?
+ Are there adult themes?
+ Can players share content with each other?
+ Will the child be exposed to inappropriate or adult themed content through other players?
+ How do players interact and communicate with each other?
+ Are players flaming and using a high amount of profanity?
+ Does the game use loot boxes or in-app purchases?
+ Are there variable rewards used to encourage gameplay to progress in the game?

Whether your child uses a console, PC, tablet or smartphone to play games, there are some essential rules which need to be clearly set out. Regardless of whatever device your child uses, you'll have to set up parental controls. All platforms have a range of choices and aren't too difficult to set up. Ensure you set up age restrictions, as this prevents the child from downloading content which isn't appropriate for their age. There are options that require you to give permission before the child can download any game or app. This is a useful tool to monitor what your child is trying to access. It also allows you to discuss why the game may or may not be appropriate for your child. The more communication and discussion you have with them regarding any online activity, the better.

"Regardless of whatever device your child uses, you'll have to set up parental controls."

If you have any doubt about a game that your child is looking to play, take the time to play it yourself. Many of the popular ones are now free to play. Giving free access to a game such as Fortnite might seem like a crazy business model. However, it's based on the concept that if the company can ensure players constantly get new content, friendly competition, and a cool social experience, players begin to invest more of their time - and money - in the game. Fortnite's big draw, for example, is spending VBucks to get new skins, dance moves, weapons, and more, making them unique from any other players. And with new daily and weekly challenges, there's an incentive to keep playing the same game ad infinitum. This system keeps players playing and spending, much to the delight of the game developers.

" It's quite possible there may be negative long-term impacts on children who are over-exposed to sexualised content. It may encourage them to explore the world of pornography."

Just like exchanging our use of social media for free for data, free games cost you in other ways. How much money do you give your children when they want to buy skins, weapons, or resources? The more a player becomes invested in the character or game they play, if maladaptive gaming is identified, it'll make quitting the game even more difficult. Everything in moderation.

We would also ask parents to be mindful of the sexualisation of female characters in games. It can't be good to set such unrealistic expectations for both boys and girls. Even beyond that, some of it is just overtly sexual. This is because the main audience of video games is actually men over the age of 18. So content is designed to appeal to the masses. It's quite possible there may be negative long-term impacts on children who are over-exposed to sexualised content. It may encourage them to explore the world of pornography.

For women and girls, the sexualisation of female characters in games - and the sexual objectification they experience in social media, magazines, movies, and TV - may lead them to judge themselves harshly. It's an impossibly unfair comparison to compare yourself with millions of others online. Young girls are currently being psychologically assaulted from every direction, by both traditional and new media platforms. It's an idealised look and body type, which is unattainable to the great majority, constantly being pushed upon vulnerable children and teens. Adults are susceptible to these external pressures also. This pressure can take an extremely detrimental toll on an individual's self-esteem over time. Ultimately, it can lead to negative body image comparisons, body dysmorphia, anorexia, social anxiety and other negative psychological consequences, or maladaptive behaviours such as self-harm.

PlayStation Network (PSN)

The PlayStation Network, simply known as PSN, is the PlayStation's gateway to online gaming. Without an account, you can't play games online - it's as simple as that. So if your child is itching to e-meet up with their friends, they're going to need one. But to create it, you must be over 18. Once you've created an account for yourself, then you can then create sub-accounts for your children which are then linked to your own. This allows you to have full control over the various parental restrictions which can be placed on this sub-account, restricting how your child can interact across the platform. As you've probably guessed, creating your own PSN account is a prerequisite for setting up parental controls on all PlayStation devices.

Restrictions available:
+ Chatting
+ In-app purchasing
+ Internet browser access
+ Inappropriate content

If you want to know how to set up a PSN account and add your children, here's what you have to do.

Setting up a PSN account
+ Go to https://www.playstation.com and click on sign in in the top-right corner.
+ Select **create new account.**
+ Enter all of your details as appropriate. Follow the steps to create your own account.
+ Now you have an account, you can **sign in.**

Adding a family member
+ Once you've signed in, click on your **profile picture** in the top-right corner.
+ Select **account settings.**
+ On the left-hand menu, click on **family management.**
+ Select **set up now** to add a new family member.
+ Click on **add a child.**
+ Enter your child's details when prompted on the screen. You can use your own email address for their account if you wish.
+ You will also have to select a **username** and **password** to protect their account. Once completed, select **I agree.**
+ To verify the sub-account that you've created, you need to open up the email account you have used to sign the child up with, open the email, and click on the link attached.

Setting a time limit on a child's account
Parental controls can now be set up for your child's account. You can set up play time to limit the amount of time they're allowed to play. This can be fixed every day, or adjusted to differ on various days of the week.
+ Go to the **family management** screen mentioned above.
+ Select the **child's account.**
+ Go to **play time settings** and adjust as you wish.

Age level for games
This option allows you to limit what games your child's account can play. These range from level 1 - the most restrictive setting - to level 11 - the most lax setting. Each level has an age associated with it, so you can limit it based on how old they are.
+ Go to the **family management** screen mentioned above.
+ Select the **child's account.**
+ Go to **age level for games** and adjust as you wish. Not all ages are represented, so we recommend you choose the one with the next closest age, rounded down.

Age level for Blu-ray discs and DVDs
This is similar to the above, but for movies and TV shows. Here you can set the age restriction or content level for playing a DVD or Blu-ray. You can also select the country or region for parental control. This refers to the age rating system set in that country.

+ Go to the **family management** screen mentioned above.
+ Select the **child's account.**
+ Go to age level for Blu-ray disc and DVD videos and adjust as you wish.

For brevity's sake, we're going to run through the rest of the options available. All are worth you looking at closely - this isn't us saying you can just scan through them. All of these can be accessed from the family management link mentioned earlier.

Use of PlayStation VR
The use of the PlayStation VR headset is not recommended for children under the age of 12. This option can be turned off by selecting the **not allowed** option.

Use of the internet browser
We recommend that you don't allow the use of the PlayStation internet browser. This option can be turned off by selecting the **not allowed** option.

Communicating with other players
Prevent chatting or messaging with players (including your child's friends) on PSN. This option can be turned off by selecting the **not allowed** option.

Viewing content created by other players
Prevent the display of videos, images, and text created and shared by players on PSN. This option can be turned off by selecting the **not allowed** option.

Monthly spending limit
You can limit the total amount your family member can spend on content in a calendar month. Regardless of this setting, funds can only be added to this wallet by you. You can leave this option at £0 or set a limit.

PlayStation 4

The PlayStation 4 - or simply just the PS4 - is one of the biggest consoles out there, having sold over 114 million units. Ever since they released the PS1, Sony has been at the top of the console market, and its legacy is something to behold. Given all the decades they've had, it's nice to see them integrate a full suite of parental controls. If you didn't read the previous chapter, you'll need a PSN account of your own to set these restrictions for your child. So give that a read through before you begin with this chapter. Once you've done that, you'll be able to change settings from your PC, the PS4 console, or even a tablet or smartphone.

Restrictions available:

+ App access
+ Game ratings
+ Inappropriate content
+ Online games
+ Privacy and identity theft
+ Purchasing options
+ Location sharing

We have plenty of options to run through, so get ready for a lot of work!

Setting up parental controls on the PS4

+ Firstly, you need to have an existing PSN account. If you don't have one, follow the steps in the previous section to create one.
+ Now you can log into the PS4 using your PSN account.
+ To access the main menu, press the up button on the PlayStation controller and move along to the right through the various options until you highlight the **settings** icon.
+ Press the **X button** to open the **settings** menu.
+ Scroll down through the options and select **parental controls/family management.**

There's a lot we recommend you do, so let's run through this in stages...

PS4 system restrictions

+ Select **PS4 system restrictions.** You'll be prompted to enter a PIN for the system; the default **PIN** is **0000**.
+ Once the **PS4 system restrictions** option is open, select **change system restriction passcode** to change the system default passcode to something you'll remember.
+ You need to select **new user creation and guest login**. It's necessary to block the creation of new profiles as the parental controls you're setting up will not apply to a new user.
+ Now select the **default parental controls** option by pressing the **X button**, to create restrictions on the entire console. Press the **O button** to return to the **parental controls/ family management** menu.

Family management

+ Next, select the **family management** option by pressing the **X button.** Sign in using your account. This account is known as a **parent account.**
+ Select the **set up now** option. If you have not verified the email address associated with your new **PSN account,** you'll need to do this. Be sure to check the **spam folder** just in case it's there.
+ Once you've verified your **account**, select **already verified** and then **continue**.
+ Click on **create user** and enter your child's details.
+ Select **next** and then **accept**.
+ You can also add an existing account that your child may have or select who you want to add to your family from any accounts currently signed into the device.

Once you've created a profile for your child, or added them by entering their account details, select the profile. You'll see a new menu with a number of options.

Parental controls - play time settings

Change play time for today
Here, you can add or reduce the time your child is allowed to use the console for today.

Play time settings
This is where you can set daily restrictions on how long your child can use the console. This can be a fixed amount, such as 2 hours every day, or you can adjust it for different days of the week, allowing you to potentially give them some more time on the weekends. When their daily allowance is up, you can either have it notify them (but allow them to continue) or it can log out of the console until their restriction resets.

Parental controls - applications/devices/ network features

Age level for games
This option allows you to limit what games your child's account can play. These range from level 1 - the most restrictive setting - to level 11 - the most lax setting. Each level has an age associated with it, so you can limit it based on how old they are.

Age Level for Blu-rays and DVDs
This is similar to the above, but for movies and TV shows. Here you can set the age restriction or content level for playing a DVD or Blu-ray. you can also select the country or region for parental control. This refers to the age rating system set in that country.

Use of PlayStation VR
The use of the PlayStation VR headset is not recommended for children under the age of 12. This option can be turned off by selecting the **not allowed** option.

Use of the internet browser
We recommend that you don't allow the use of the PlayStation internet browser. This option can be turned off by selecting the **not allowed** option.

Parental controls - Network features

Communicating with other players
Prevent chatting or messaging with players (including your child's friends). This option can be turned off by selecting the **not allowed** option.

Viewing content created by other players
Prevent the display of videos, images, and text created and shared by players. This option can be turned off by selecting the **not allowed** option.

Monthly spending limit
You can limit the total amount your family member can spend on content in a calendar month. Regardless of this setting, funds can only be added to this wallet by you. You can leave this option at £0 or set a limit.

Nintendo 3DS

Nintendo hit on a genius idea when they decided to take the gaming experience handheld. The Game Boy was a massive hit in the 90s and Nintendo have practically dominated that part of the market ever since. Today, they're still going strong with their handheld console, the 3DS. It might be a smaller package, but it's still capable of connecting to the internet, so you'll need to change some of the parental control options. There are only a handful, but well worth doing.

Restrictions available:

+ Browser access
+ Game ratings
+ Inappropriate content
+ Online chat
+ Purchasing

So where do you start when it comes to the Nintendo 3DS?

Setting up parental controls account

+ When you turn the device on, it should automatically be on the **home menu**. If not, press the home button on the device itself.
+ Select the **system setting**s icon - it looks like a wrench.
+ Open the **parental controls** option and follow the on-screen instructions.
+ When prompted, enter a **4-digit PIN**. This prevents settings being changed.
+ Confirm the **4-digit PIN** twice!
+ When prompted, select a secret question and answer. This is to assist you if you forget the **4-digit PIN.**
+ When asked to **register an email address,** ensure it's not one the child will have access to.
+ The email address, along with the **4-digit PIN**, can be used to access the **parental controls.**

Setting up parental controls for game ratings, internet access, and purchases

+ When you turn the device on, it should automatically be on the **home menu**. If not, press the home button on the device itself.
+ Select the **system setting**s icon - it looks like a wrench.
+ Open the **parental controls** option and follow the on-screen instructions.
+ When prompted, enter your **4-digit PIN.**
+ By default, all parental control options are enabled and can be changed according to your child's needs under **software rating, internet browser, shopping services**. We won't go through them all as they're quite self-explanatory - just change as you wish.
+ Once you have chosen the appropriate settings, select **done** to confirm.

Nintendo Switch

PlayStation might be the big kid on the block, but you'll be hard-pressed to find anyone with as strong a legacy as Nintendo. The likes of Atari and ColecoVision might be the grandfathers of home consoles, but Nintendo were the ones who came along and changed the game with the Nintendo Entertainment System (NES). Today, over 35 years later, they're still going strong.

Restrictions available:

+ Age ratings
+ Internet browser access
+ Inappropriate content
+ Online chat
+ Time limits

One of the most popular gaming platforms for children, the Nintendo Switch thankfully has a good variety of parental controls you can avail of.

Setting up parental controls using the console

+ On the home screen select the **system settings** option. This can be done both if the device is docked or if you're holding it. If it doesn't automatically go to the home screen, press the home button on your controller.
+ Scroll down the left-hand bar and select the **parental controls** option.
+ Then select **parental control settings** on the right-hand side of the screen.
+ Two options for parental controls now become available.
+ Select the **'set with this console'** option.

At this point, you'll have access to a variety of options. Let's run through what's available to you:

+ **Restriction Level**
  - » This is an overall setting. If you don't feel the need to go through each setting individually, you can set blanket restrictions based on their age group - young child, child, or teen. If you want, you can choose the custom option to change each setting individually.
+ **Restricted software**
  - » You can set a restriction on software based on your child's specific age.
+ **Content rating system**
  - » This is the rating system for your particular country. It should already be set to the correct one.
+ **Posting screenshots/videos on social networks**
  - » This is simply an on or off situation. As the Switch can connect to social media like Twitter to post content, it's a necessary feature.
+ **Free communication with others**
  - » Here, you can set communication restrictions on a per game basis.
+ **VR mode (3D visuals)**
  - » Certain games have VR modes; use this to restrict that option. Again, it's an on/off situation.

Setting parental controls using the Nintendo Switch Parental Controls app

+ Download the **app** from the **app** store on your device.
+ **Open the app** and follow the onscreen instructions in creating a Nintendo parent account.
+ Once set up, you'll need to connect your Nintendo account and the Nintendo Switch account on the console.
+ **Enter the code** to pair the console and the smartphone.
+ Once the devices are linked, you can use the app to set the content restrictions. All of theones above can be changed on the app too. But by using the app, there are a couple more options open to you:
  1. **Restricting purchases** - If you connect a child account, you can stop them from buying content from the Nintendo eShop.
  2. **Time limits** - You can impose time restrictions on how often your child uses the console.

Nintendo Wii

The Nintendo Wii might have come out all the way back in 2006, but it's an enduringly popular console. Thanks to its novelty Wiimotes that let you flail your arm around to play a game of tennis or bowling, kids still love it. So if you have one lying around, it might be worth setting up the parental controls just in case it sees some use.

Restrictions available:

+ Age ratings for games
+ Inappropriate content
+ Online chat
+ Search engine access
+ Time limits

For a console that's 15 years old, it has a decent range of parental control options available to you.

Setting up the parental control

+ In the **Wii menu**, select the **Wii icon** in the bottom left of the screen.
+ On the next screen, select **Wii settings.**
+ Highlight the **Wii system settings** menu and move right to select **parental controls.**
+ Read the content on the following screens and select **confirm**.
+ When prompted, enter a **4-digit PIN** - this will be used to access the parental controls.
+ Next, complete the **secret question** in case you forget your PIN.
+ On the **parental controls** screen, select the **game settings and PIN** option.
+ Then select the **highest game rating allowed option.**
+ Now select the age rating for games that are permitted on the console according to your child's age.
+ Select **OK** to review your settings, and then **confirm**.

Setting the various parental controls

+ On the **parental controls** screen, select **other settings.**
+ You will be presented with a variety of options:
  - » **Restrict purchasing**
  - » **Messaging**
  - » **Access to the Internet Channel**
  - » **Access to the News Channel**
+ Set each one according to the needs of the child.

Nintendo Wii U

The Nintendo Wii U is the successor to the Wii, though it wasn't quite as popular. It eschewed the Wiimotes for a controller with an in-built screen - it doesn't look too dissimilar to their recent Nintendo Switch! But while it might not have made its way into as many homes as the Wii, it's still a multi-million selling console, one children love.

Restrictions available:
+ Age ratings
+ Internet browser access
+ Inappropriate content
+ Online chatting
+ Online and in-game spending
+ Time limits

What can you as a parent change about the Wii U? Well, much like its predecessor, there's a nice collection of settings you can change.

Creating your parental control PIN
+ On the **Wii U menu**, select **parental controls.**
+ Read the following messages by selecting **next** or press the **A button** on the controller to dismiss them.
+ When prompted, enter a **4-digit PIN** and select **OK.**
+ Next, select a **secret question** that will be used in case you forget your PIN.
+ Enter an email address and select **next** or press the **A button** and complete the registration.

Setting up parental controls
+ On the **Wii U menu**, select **parental controls.**
+ Enter your **4-digit PIN.**
+ When the parental controls screen opens, use the **arrows** or left and right on the **d-pad** to select which restrictions you wish to apply.
+ Select the user and navigate through the various settings, which include:

Internet Channel
You can permit or restrict use of the browser. We recommend restricting it.

News Channel
You can permit or restrict access to the News Channel.

Wii messages
Wii U consoles can only send and receive messages if both of the users have entered each other's unique numbers in their address books. You can disable the console's ability to send and receive messages from other people. System updates will still be received.

Use of Wii Points
You can permit or restrict access to Wii Points. These are used to acquire downloads from the Wii Shop Channel. If this setting is on, users will be required to enter the 4-digit PIN to use Wii Points.

+ Select the particular settings you wish to change or press the **A button.**
+ To save your choices, select the **back** option or press the **B button** to exit and save your changes.
+ The **4-digit PIN** number will be required if the user tries to access content that's now restricted.

Xbox 360

Microsoft isn't just a computer OS provider. They shocked everyone when they burst their way onto the console scene with the original Xbox. It managed to sell 24 million units, but it's follow-up - the Xbox 360 - blew those numbers away. The Xbox 360 sold a whopping 84 million units and became a new staple console goliath. It may have been released in 2005, but there's every chance you still might have one hooked up in your house.

Restrictions available:

+ Age ratings
+ Online chat
+ Inappropriate content
+ In-app/game purchasing
+ Internet browser access

As old as the console may be, it has an impressive suite of parental controls.

Setting up parental controls

+ From the home screen, select the **settings menu.**
+ Then select the **family** option.
+ All of the accounts registered on the device will appear here.
+ Move across the screen and select **content controls.**
+ Activate the parental controls menu by switching it **on**.
+ You can customise your parental settings according to the needs of the child. The options available include:
    - » **Ratings and content**
    - » **Family timer**
    - » **Xbox LIVE access**
    - » **Xbox LIVE membership creation**
    - » **Change pass code**
    - » **Reset to default settings**
+ Select **save and exit.**
+ You'll be prompted to create a **pass code** and **pass code question.**
+ Then select **save and exit again.**

Setting up privacy and online settings

+ From the home screen, select the **settings menu.**
+ Then select the **family** option.
+ All of the accounts registered on the device will appear here.
+ Select the **user account** you wish to apply the setting to.
+ Now select the **privacy & online** settings section.
+ At the bottom of the block, select **change settings.**
+ A number of options will be available:
    - » **Adult**
    - » **Teen**
    - » **Child**
    - » **Custom**
    - » **Customise**
+ Select the appropriate age profile for the user. This will change all settings to match the age.
+ If you want to change every setting yourself, hit the customise option.
+ You can select the appropriate privacy and online settings under the following areas:
    - » **Online gameplay**
    - » **Friend requests**
    - » **Purchase content**
    - » **Video communication**
    - » **Web browsing**
    - » **Profile sharing**
    - » **Kinect sharing**
    - » **Social network sharing**
    - » **Game activity**
    - » **Friends list**
    - » **Voice data collection**
+ Once the appropriate selections have been made for your child, select **save settings.**

NOTE - It can take a few hours for the selected settings to come into effect.

Xbox One

We won't blame you for getting a bit confused with this one. Despite being called the Xbox One, this is **not** the first Xbox released. In fact, it's the sequel to the Xbox 360. Released in 2013, it wasn't as popular as its predecessor, but still managed to clock in at 54 million sales. With the release of the Xbox Series X (the latest iteration) having only just happened, this will likely still be the main console in many households.

Restrictions available:

+ Age ratings
+ Inappropriate content
+ Internet browser access
+ Online purchasing
+ Online chat

Let's take a detailed look at how to make your child's XBOX safer.

Setting up parental controls

+ On the Xbox One dashboard, select the **settings** option.
+ Then select **privacy & online safety** where a number of options will be available:
    - » **Child defaults - more private**
    - » **Teen defaults - moderate**
    - » **Adult defaults - more social**
    - » **Custom**
+ To restrict all adult content for a young console user, select **child defaults.**
+ The **content restrictions** include:
    - » **Access to content**
    - » **Web filtering**
    - » **Descriptions in OneGuide – explicit text**
    - » **Contact preferences**
+ You also have the option to select **custom** to customise the settings according to the specific needs of the child.
+ On the **child and online safety summary** page that opens, you'll have two options:
    - » **Use for [your child's username]**
    - » **Use, but customise**
+ Select **use, but customise.**
+ On the **Customise privacy and online safety for [your child's username]** page that opens, there are several default privacy settings, such as:
    - » **Buy and download**
    - » **Join multiplayer games**
    - » **Use video for communications**
    - » **Content and apps**
    - » **And so on...**
+ Select the relevant options according to the specific needs of the child.
+ Ensure you review the settings under **content and apps.**
+ Select **access to content and apps menu** to set the age ratings for content accessed on the device.

Xbox Live

Xbox Live is Microsoft's equivalent to the PlayStation Network. To play games online, you need a subscription to Xbox Live. And since many of the most popular games with kids - such as Fortnite or Apex Legends - are online-only, your child may well want a subscription. But, as we talked about before with unsavoury people having access to your child, you want to ensure they are as safe as possible.

Restrictions available:

+ Age ratings
+ Inappropriate content
+ Internet browser access
+ Online chat

It may not be a physical platform like the Xbox One, but there are still some changes you can make to Xbox Live.

Setting up parental controls for accessing certain content

+ Go to https://www.xbox.com on an internet browser.
+ On the homepage, select the **person icon** at the top right of the page.
+ If you haven't already **set up an account**, follow the onscreen instructions to create one.
+ **Sign in** to Xbox Live using your **email address** and **password.**
+ Select the option for **account.**
+ Then select **security, family and forums**.
+ Select **access to content** to set the appropriate age restrictions for game and website access.

Setting up parental controls for privacy

+ Go to https://www.xbox.com on an internet browser.
+ On the homepage, select the **person icon** at the top right of the page.
+ If you haven't already **set up an account**, follow the onscreen instructions to create one.
+ **Sign in** to Xbox Live using your **email address** and **password.**
+ Select the option for **account.**
+ Then select **privacy settings.**
+ Select the appropriate protection level in each category according to what your child needs.

Some advice to parents on cyberbullying

Cyberbullying continues to exist as one of the darkest parts of the online world. It really doesn't matter who you are, you're always only a single text, message, or post away from becoming a target. The number of lives that have been lost globally due to cyberbullying are staggering. Families, loved ones, and friends are very often left completely broken when a person decides to take their own life due to being targeted online. The greatest difference between offline and online bullying is that there's no safe place. Home is no longer a sanctuary because the cyberbully exists in the devices you carry in your pocket or use at home. It's constant, unrelenting, and can be difficult to escape if you don't know what to do.

Over the last few years, we've seen kids of all ages rush to social media, gaming, and messaging apps to be part of the conversation. But when they become a target, the fun stops. In a world where technology is actually isolating people even further under the guise of being constantly connected, cyberbullying can feel truly segregating and devastating. We've even seen kids become the cyberbullies themselves, fearing they'll be the next victim and trying to be "part of the gang". It's a learned behaviour to keep themselves safe, but it's still wrong.

Beyond that, why do people cyberbully others in the first place? The simplest answer is there is every reason, yet no reason at all. We've seen examples over the years ranging from simply just not liking a person, to thinking they deserved it, to the perpetrator just trying to be noticed and accepted by their own peers. However, while the reason to target someone may vary, the feeling they get will be the same. They'll get what they want - that feeling of power and being in control - and that just pushes them to keep it up.

As parents, we have to accept that there's no shortage of simply misguided or just downright bad people in the world. Every one of them can access the internet as well. When we make a decision to give our children access to the online world, we have to understand and take ownership of the fact that, for the most part, the online world is unregulated, and anything goes in what is essentially an adult environment. Yes, there's content specifically created for children to explore, however there are no rules here. Often, the comparison is made to the Wild West, and while some protective structures do exist, it's an unsafe space for children to be left to explore alone.

"Parents need to remember how much time young people invest in their online lives."

If we do choose to let our children access the online world, we should do so in a safe, monitored, and restricted way. It won't entirely guarantee a person's safety online, but it will go some way to protecting them. We'd like to see parents take on a more engaging role with children when they venture online. Helping a child to develop a strong resilience and the ability to view content targeting them as an unpleasant inconvenience rather than becoming upset by the content. Learning to appropriately deal with it and then move on. As cyberbullying for the most part takes place in a very public environment, it does require a considerable level of resilience to be able to cope.

We've met teens who, despite being targeted online and suffering torrents of abuse, still choose to remain on the platform. Why? Because a single person in their online circle of friends or followers sent words of encouragement to them. The victims hold onto this connection as a reason to stay immersed in an otherwise completely abusive realm. The psychological harm inflicted on people who are suffering from cyberbullying can be enormous. Parents need to remember how much time young people invest in their online lives. In a world where some view it as more important than their real life, an attack on that person's online persona can have far-reaching consequences.

There are a number of different approaches to cyberbullying. Sometimes it's just a simple message that cuts deep. Or maybe it's specifically being excluded from a group of 'friends'. Some people might catfish them, posing as a new friend just to get access to their content and embarrass them with it. Anything where the sole intention is just to kick someone while they're down - and they're all terrible.

And online gaming is just as much a breeding ground for this type of abuse. Maybe even more so. It's all too easy for someone to spit vitriol at you based on your skill, telling you to "kill yourself" for the mistake of dying in a video game. Almost all platforms have a way to report the abuse. Parents need to familiarise themselves with how to use these features and then teach their children the same. Informing a parent or another trusted adult, saving the content, blocking, and reporting need to become second nature for children. They need to have the confidence to know that using these features is the right course of action. They also need to be comfortable with discussing every experience they have online with their parents. Sometimes the cyberbullying might be embarrassing to the child, so much so they may not want to discuss this with their parents. So having an appointed trusted adult other than a parent can be very helpful if this happens.

Parents also need to teach children what engaging with the online gaming world means. Essentially, you're asking a planet full of people to judge you. Nobody would do this in the real world. Can you imagine walking into a crowded room filled with thousands of strangers and saying, "I know none of you know me, but I want you to judge me. Tell me what you think of me"? If you don't create an opportunity for a person to judge you, then they simply can't.

And not everything we do needs to go online. Parents are possibly the greatest offenders here. Some parents post an absolutely ridiculous amount of images of their children online. We have to always be mindful that we lose all control of content once it's posted online. You have no idea who will see and use these images.

We all have embarrassing pictures from when we were kids. As adults, we can look back and laugh. Stick it on a cake and it's even more hilarious. But for a self-conscious teenager? That's practically the end of the world. What happens if a cyberbully gets hold of that image and uses it for wanton terrorising of your child? You should always ask for your child's permission first before posting anything about them online.

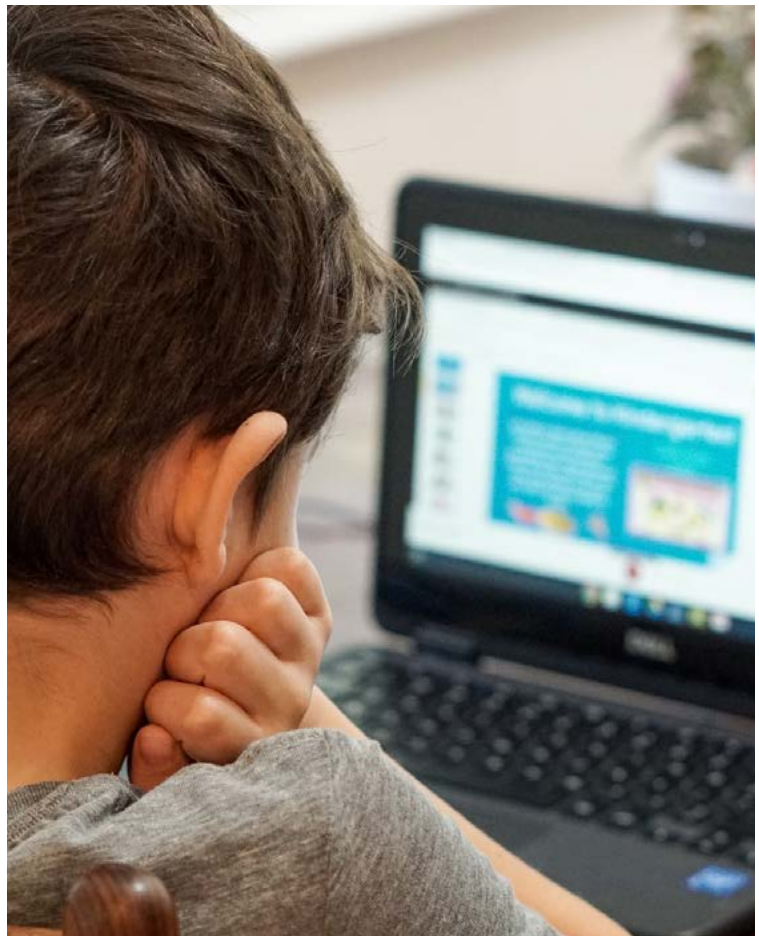
It's important that parents learn how to identify if their child is a victim of cyberbullying. Statistically speaking, children are unlikely to tell their parents if it's happening. Most parents will discover it when a teacher, relative, or family friend brings it to their attention. Having access to a digital device means responsibility. Part of that responsibility means there can be no secrets or fear in telling a parent what's happening online. If you do discover your child is being targeted, remain calm. They'll look to you to see how they should react. If dealt with in a calm, structured approach, they're more likely to come to you if it happens again.

You want your message to be loud and clear: they need to stop and don't engage any further. The last thing you want is to give the cyberbully any attention. "Don't feed the trolls" as they say. Screen capture or use another device to take pictures of the harmful content. Report the user to the platform host and, if necessary, the Data Protection Commissioner and legal authorities, before you then **block the user.**

If you do go down a legal route, be aware that there may be a number of stumbling blocks which put many people off following through with their complaint.

Firstly, it takes time. It can be a considerable length of time in fact. So don't expect immediate results. Secondly, while we highly recommend making a complaint to the authorities, the safety and wellbeing of the victim is paramount, which is why they may need to avoid the platform until the situation is resolved. If the cyberbully is known to you, don't engage with them if you make an official complaint. We have seen this happen; everyone falls foul of the authorities, especially if things get out of hand. Know that each digital device has its own individual identification known as a MAC address. Upon signing up for an account, this number can be linked to the account. Content that's deleted isn't gone forever. It may still exist on a company server or on the offending device itself for a long time, so don't worry if a person tries to hide what they've done. Have patience. It's a very difficult thing to ask for, however these matters are resolved in many cases, but they just take time.

Regardless of how you and your child decide to approach cyberbullying, always ensure that their emotional and psychological wellbeing are treated as a priority. Seek help for them if you feel it's necessary. But always ensure that, above all, they're always your number one.



10

Online gaming

Fortnite

Fortnite: we had to have a chapter on it eventually, didn't we? If you have a child anywhere between 6 and 16, they probably want to play Fortnite. It's a game where you - and potentially a team of friends - try to survive a battle royale of everyone trying to eliminate one another. The last person standing is the winner. It's a relatively cartoony take full of strange costumes and dances and, as far as the content goes, is fairly harmless. But since this is an online-only game, and a competitive one at that, it can bring out the worst in people. In your own child, it could bring out an angry side in them. Outside that, others might use the space to troll or harass your child. So you do have to be careful; don't let its whimsical animated look deceive you.

Restrictions available:

+ Inappropriate content
+ Online chatting
+ Hide profile

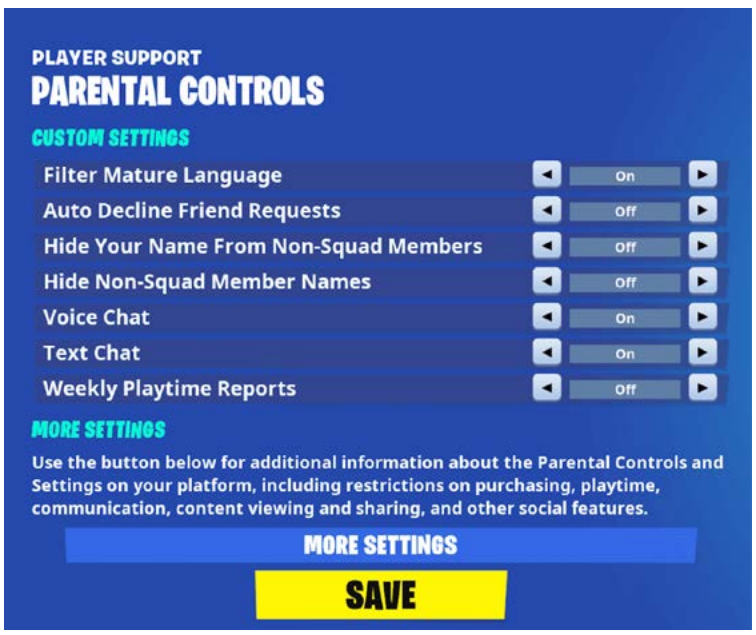
Fortnite offers a wide range of parental controls that can change what players do and see within the game. Additional controls may be set on PlayStation, Xbox, Nintendo, and iOS platforms themselves.

How to open up parental controls

+ Launch **Fortnite** on the device.
+ Select the **menu** in the upper right of the screen.
+ Then select **parental controls.**
+ If there's no email address linked to the account, follow the on-screen instructions.
+ If there is, then enter the **email** details.
+ When prompted, enter a **six-digit PIN**. This is needed to make any changes to parental controls in the future.
+ If the **six-digit PIN** is changed, an email to notify of the change will be forwarded to the email associated with the account.
+ In the event you forget the **six-digit PIN**, you can contact **player support** to recover it.

Parental controls available

+ A list of the available controls can be seen in the image. Once you've made the appropriate changes to the settings, select save to complete setting the parental controls.



Filter mature language

Text chats are available within the game with known and unknown players. There are two options:

+ **On** - Mature language filtered and replaced with heart symbols in text chat.
+ **Off** - Mature language appears in text chat.

Auto decline friend requests

By its very nature, Fortnite is a social game. It's possible to play with existing friends and make new ones. Receiving friend requests can be set to:

+ **On -** Receive friend requests.
+ **Off -** Do not receive friend requests.

You can also set the level of interaction with players who are accepted as friends by selecting the player and choosing one of the following:

+ **Whisper** - Communicate with the player in private messenger.
+ **Unfriend** - Remove a player as a friend.
+ **Block** - Block a player from being able to interact any further.

Hide your name from non-squad members
The account names of players who are eliminated in the match appear on the screen. This setting will replace the profile name with 'Player' for everyone outside of the squad (the group of friends you're playing with):

+ **On** - Display **'Player'** to players not in your squad.
+ **Off** - All players see the profile name.

Hide non-squad member names
You can do the same with other players' names:

+ **On** - Replaces the names of players not in the squad with **'Player'.**
+ **Off** - All profile names are visible.

Voice chat
Unless this setting is changed, the default is for an open level of communication between teammates and the other users. It's an important setting for parents to set as it controls whether or not the user can interact with others verbally. Note that there are no restrictions or controls to prevent hearing inappropriate content:

+ **On** - The user can hear teammates and talk to them.
+ **Off** - The user cannot hear or talk to teammates.

Text chat
While in a party with friends or when teamed up with random players during a match, a text chat channel becomes available. This setting controls whether or not this account can receive or send messages in the text chat channel.

NOTE: This setting disables Fortnite's in-game text chat. The platform you're playing on may have additional communication features that must be restricted separately. For information on platform specific controls, use the **more settings** option:

+ **On** - You can send and receive text chat messages with your teammates.
+ **Off** - You cannot send or receive text chat messages with your teammates.

Weekly playtime reports
This is an essential aid for parents to keep an eye on how much time their child is spending playing Fortnite. Once activated, a weekly playtime report will be forwarded to the email address associated with the account:

+ **On** - Send a weekly report.
+ **Off** - No reports will be sent.

More settings
Under this option setting, you'll find options for:

+ In-game purchases
+ Sharing content
+ Playtime restrictions
+ Content restrictions
+ Social media

Reporting another player
Using this option might be a matter of when, not if. Remember what we said in the previous section: teach your child how to use the report function liberally.

+ Find the player you want to report.
+ Then select the **report** option.
+ The **send feedback** form will open up which allows the user to enter the details of what occurred in the game.
+ Players who are found to be in breach of the terms and conditions of Fortnite will be banned from the game.

Important note for parents
Depending on the parental controls you've set on the console or platform being used, you'll have to consider whether you've set the same settings in the game. If you restrict some aspects in the game but permit it on the platform, then the child may still be able to do any of the following:

+ In-game purchasing
+ Communicate with other players
+ Change play time
+ Add friends
+ Broadcast gameplay
+ Alter which games can be played and downloaded
+ Change what content can be seen and shared
+ See more about other players
+ Access web browsing

Note for parents of children using Android devices
On Android, you can use the in-game Fortnite parental controls to restrict or allow specific types of behaviour. **The Google Play parental controls do not apply to Fortnite.** In-game purchasing restrictions for Fortnite on Android are available via a PIN restriction.

Epic Games Store

If your child wants to play Fortnite on their PC, then they'll need to use the Epic Games Store. That's because Epic Games, the makers of Fortnite, also own this storefront and have made Fortnite exclusive to it. So you can't have one without the other. ***Note: this doesn't affect consoles.***

Restrictions available:

+ In-game purchases
+ Game and content restrictions

There are two ways you can go about setting up parental controls. You can do it from within the Epic Games Store launcher or, if you don't have access to that PC, you can do it from any browser on the Epic Games Store website.

How to set up parental controls using the Epic Games Store

+ Open the **Epic Games Store launcher** and log in with your **email** and **password**.
+ At the bottom-left corner of the screen, select the **account name.**
+ Then select **manage account.**
+ Scroll down and select **parental controls**.
+ You'll be prompted to enter a **six-digit PIN.**
+ You can now set up a **PIN requirement for purchases** and set a **restriction on access to games**, including free games.
+ Select **save** to finish.

How to set up parental controls using a web browser

+ Go to www.epicgames.com/store
+ In the top-right corner of the screen, select **login**.
+ From the drop-down menu on your **account name**, select **account**.
+ Then select **manage account.**
+ Scroll down and select **parental controls.**
+ You will be prompted to enter a **six-digit PIN.**
+ You can now set up a **PIN requirement for purchases** and set a **restriction on access to games**, including free games.
+ Select **save** to finish.

Roblox

Roblox is a massive multiplayer online gaming global platform. Yes, we used the term 'platform'. That's because Roblox goes beyond a game; millions of users use the platform to imagine, create, and share experiences with each other in immersive, user-generated 3D worlds. It's one of the most popular platforms for children under 12 years of age and is available on PC, mobile devices, and the Xbox One. It's free-to-play, much like Fortnite, and has its own in-game currency - Robux. So with access to other people around the world and open monetisation, this is a game where you'll have to keep your eye on what your child is engaging with.

Restrictions available:

+ Online chat
+ Inappropriate content
+ Game restrictions
+ Inappropriate behaviour

There's a lot we recommend you change to keep your child as safe as possible.

Setting up two-factor authentication

+ Go to https://www.roblox.com/
+ If your child already has an account, **log in** using their **username** and **email address.**
+ If you don't already have an account, select **sign up** and follow the onscreen prompts.
+ **Verify** your email address.
+ On the home screen, select the **cog icon** in the top-right corner of the page.
+ Select **my settings.**
+ Choose the **2-step verification** option and activate by switching it on. A code will be sent to the email address connected with the account to complete the login from now on.

How to turn on the parental PIN

+ Go to https://www.roblox.com/
+ On the home screen, select the **cog icon** in the top-right corner of the page.
+ Select **my settings.**
+ Select **security**.
+ Activate the **Parental PIN.**
+ Enter a **4-digit PIN** when prompted.
+ Select add to **save**.

How to enable account restrictions

+ Go to https://www.roblox.com/
+ On the home screen, select the **cog icon** in the top-right corner of the page.
+ Select **my settings.**
+ Select **security**.
+ Activate **account restrictions.** Now the account will only access curated content on the platform. Additionally, contact settings will be set to **off.**

How to restrict in-game contacts and messages

+ Go to https://www.roblox.com/
+ On the home screen, select the **cog icon** in the top-right corner of the page.
+ Select **my settings.**
+ Select **privacy settings.**
+ Then select **contact settings.**
+ If you have activated the **parental PIN**, you'll be prompted to enter it.
+ You can now select **custom** and set the contact settings to meet the needs of your child under the following headings:
    - » **Who can message me?**
    - » **Who can chat with me in the app?**
    - » **Who can chat with me?**

+ The options for each are:
    - » **Friends**
    - » **Everyone**
    - » **No one**
+ We recommend you change it to at least friends, if not blocking out everyone altogether.

Other contact settings to consider

+ There are a further three options available for parents to consider in **contact settings** under **other settings** which should be set to **friends** or **no one.**
    - » **Who can invite me to VIP servers?**
    - » **Who can join me?**
    - » **Who can see my inventory?**

How to report another user

Roblox has a **report** system which features throughout the site and also in the games:

+ To use it, head into the game and select the **menu** located in the top left-hand corner. It looks like three horizontal lines.
+ Select the **flag icon** located next to the user's name.
+ You can also just select **report** in the menu.
+ The prompt will say **"for game or player?"**
+ Select the **player** option.
+ Choose **which player** from the pull-down menu and find the username you wish to report.
+ Then select the **type of abuse** menu and choose the appropriate option.
+ If needed, additional information can be entered in the description box.
+ Finally, select **submit** to complete the report.

How to report a game

Roblox does have a strong set of rules and guidelines by which users and game developers must abide by. Should a game not meet these guidelines, select **the offending game** and follow these steps:

+ On the **about page** of the game, select the red **report abuse option** in the bottom right-hand corner.
+ Choose the appropriate **category** and fill in the **comment box.**
+ Then click **report abuse** at the bottom right of the screen.

Reporting other content

It's possible to report an item in the catalogue or library if you feel it doesn't follow the rules and guidelines:

+ Select the **three dots** in the top right-hand corner of the item's information box.
+ Then select **report item** and complete the form.

Reporting an inappropriate or offensive chat

+ Select the **gear icon** in the top right-hand corner of the chat window to open the **chat details.**
+ Click the **three dots** next to the user's name.
+ Select **report**.
+ Then select the red **report button.**
+ Complete the **report form** and hit the green **report abuse** option when done.

Steam

Steam is another platform much like the Epic Games Store. Created by Valve, Steam is seen as the platform for PC gaming. It's all-encompassing, acting as a store, game library, community hub, and online forum. As you can likely see, there are plenty of opportunities for your child to access inappropriate, adult-orientated content. There's nothing stopping them from freely interacting with strangers through the community hubs, so it's important to review these parental control settings.

Restrictions available:

+ Inappropriate content
+ Online gaming
+ In-game purchases
+ Restrict mature content

It's highly recommended that you ensure your children have a fully restricted Steam account. Here's how to adjust the settings.

How to set up Family View

+ **Create** or **log in** to the Steam account you intend for your child to use.
+ Click the **Steam drop-down menu** in the top menu bar.
+ Select the **settings** option.
+ On the left side of the window that opens, select the **family** option.
+ Then select **Family View** to begin the **Family View wizard** setup.
+ There are a variety of options available to restrict. Select the ones that are most applicable to your child. These will be **PIN-protected** if accessed in future.
+ When prompted, select and then confirm your new **PIN**.

Setting up the family games library

You can choose to only allow access to a subset of the Steam account's library. The account's library will include a new group called **family games**; these are games you've chosen to remain accessible while in Family View. To add or remove games, Family View must be disabled.

+ **Create** or **log in** to the Steam account you intend for your child to use.
+ Click the **Steam drop-down menu** in the top menu bar.
+ Select the **settings** option.
+ On the left side of the window that opens, select the **family** option.
+ Then select the **Family View** icon.
+ Now enter your **Family View PIN** number to exit **Family View.**
+ Find the game in your library and **right-click on the game** and select **add to/remove from family games.**
+ **Confirm** your selections.

How to change your Family View options

+ **Create** or **log in** to the Steam account you intend for your child to use.
+ Click the **Steam drop-down menu** in the top menu bar.
+ Select the **settings** option.
+ On the left side of the window that opens, select the **family** option.
+ Then select the **Family View** icon.
+ Now enter your **Family View PIN** number to exit **Family View.**
+ You're now able to adjust any settings as you wish.

Twitch

Twitch is a very popular online service for watching and streaming digital video broadcasts. Think YouTube, but live all the time. While Twitch originally focused almost entirely on video games, the platform has expanded to include streams dedicated to artwork creation, music, talk shows, and the occasional TV series. You can jump around between channels looking for content creators that take your fancy, many of which are likely unsuitable for children. So it's advisable that you set up a restricted account for your child.

Restrictions available:

+ Inappropriate content
+ Media streaming
+ Online games
+ Social networking
+ Access to graphic content

There isn't much you can do, but there are some blanket parental controls you can set up.

Setting up parental controls

+ Go to https://www.twitch.tv/
+ In the top-right side of the screen, select **sign up** if you don't have an account and follow the on-screen prompts to create one.
+ Select a **PIN** and re-enter it when prompted.
+ If you do have an account, select **log in.**
+ Select the **drop-down menu** at the top-right corner of the window.
+ Flip the switch next to **online**. Then deselect the **share my activity** box if you do not wish your child's content to be shared with others online.
+ Then select **settings** from the bottom of the drop-down menu.
+ Choose the **security and privacy** option.
+ At this point, it's important to enable **two-factor authentication** to protect the account.
+ Select **privacy** and click the box to **block whispers from strangers.**

Staying safe online

Throughout this book, we've covered a wide range of technology, platforms, and services that connect to the online world. And we have no doubt there was so much more we could have covered. By the time you're reading this, there might already be a new hit game or streaming service that everyone can't get enough of. But that's just the nature of the internet.

While we've done everything we can to ensure you feel confident about protecting your children, you will no doubt face new challenges we can't even predict. The difference is now you have the tools and knowledge to go out there and make them work for you. The lessons you've learned throughout this book can be applied to any platform. While the steps won't be exactly the same, we're sure you can take our advice and figure out the individual quirks of every other piece of technology. If you ever struggle with this, we're always a quick email away.

Whether you read the entire book front to back or just used it as a reference guide for the few platforms and services you use, you now know what you need to do everything you can to protect your children. Because that's what this book is all about. It isn't about being the bad guy, or the strict parent. It's about keeping them safe. The world can be a dangerous place, and the internet is no different. Children will never understand the depths people will sink to. It's why it's a parent's job to keep them safe.

That's all any parent ever wants. And if this book was your way of putting yourself out there to learn everything you need, then congratulations. You've done it. Now get out there and protect those kids!

We'll reiterate what we said at the start: the first step you need to take is to do an audit of the devices in your household, the services you're subscribed to, the platforms your children use, and the games they play. Figure out what you need to fix, make a list, and go! Your 21st-century household probably has a lot that needs changing, but all you can do is start at the beginning.

In the good times and the bad, when your kids say they hate you because you won't let them talk to their friends on Snapchat, remember why you're doing this. This book will always be here for you to come back to as a reminder of what you're trying to do.

Good luck on your journey.

A final word from Jason...

For you, mum.
You always had faith in me when nobody else did.

A special word of thanks to Dillon, Lorcan, and Eabha, my three beautiful children who ensure I stay constantly motivated to keep not only them, but every child safe online. Also, to Morgan, Sharon, Barbra, Eileen, and John, without whose support and guidance none of this would be possible.

Thank you.

Thank you