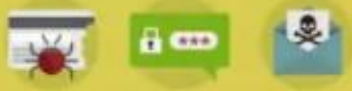




ST. MARY'S *Catholic High School, Dubai*



A PARENTS GUIDE TO

Protecting Their Kids Online



Source: <https://www.vpnmentor.com/blog/the-ultimate-parent-guide-for-child-internet/>



So many Online Child Safety guides **are just scaring parents, without telling them what they can actually do**; and it's all about steps you can take to protect your child from **Sexual predators, Cyberbullying, Mobile phone addiction, and hurtful content**.

While we don't think you should panic as a parent, you do need to be aware of the risk's magnitude, as every kid could be affected. What can we do as parents? Instead of using technology to just to keep kids occupied, we need to educate them about it. Instead of sticking phones in their tiny hands at **younger and younger ages**, we need to tell them about the dangers of online life. And instead of hoping everything will be just fine, **we need to take action**, check our kids' activity, and make sure it actually will be fine.

This comprehensive guide **will show you how**. In it, we've outlined eight areas that you should pay attention to as you navigate this complex online world – from mobile devices to social media, gaming, cyberbullying, and information security.

The usual challenge is that most parents **don't really understand** platforms like TikTok, Instagram, Snapchat and even Twitter – not to mention 4Chan and gaming communities. But for their kids, the online world is more real than the real world. **It is crucial for our children's sake that we understand what they see online**, what is out there, both good and bad, and how it impacts their physical and emotional well-being.

The good news is that **it's not that difficult to put certain technical controls in place to protect your children online**. Far more importantly, **the best thing you can do to protect your children is to talk to them**. This guide will help you set clear boundaries for what and

when they access online, but also to be there for your children when they make a mistake, or when they have gone too far. Isn't that what parenting fundamentally comes down to?

1. Mobile phones and apps

According to research by SellCell, the average age that children get their first smartphone is 8 years old and it seems to keep dropping. The average was 10 in 2015 according to 000. While giving a child a smartphone comes with some benefits, it's easy to forget they're no less than a Pandora's Box.

Smartphones give kids unprecedented freedom: The ability to **communicate with people without supervision**, to consume **whatever content they desire** and even **act forcefully** towards other kids online with ease. If they don't know how to behave with their phone, follow basic ethics and caution, and be aware of the risks – they could fall victim to **online harassment**, Malware and **money theft**, get exposed to violent or sexual content and far worse. Since smartphones are personal devices, **we don't often know** what our children do with them, how they use them, and what threats they encounter.

If you're considering giving your child a smartphone, it's critical to have some clearly outlined guidelines in place beforehand, so that everyone is on the same page. If your child already has a smartphone, it's not too late to review the family rules. Demonstrate to them that having a smartphone is a big responsibility.

There are many precautions you can take to implement phone safety:

- Have your kid sign a smartphone contract before you give them one. Print out a list of cellphone rules and stick it in a public place in your home.
- Download parental controls. Parental control apps for younger children enable you to limit your child's usage, determine their location, and monitor their calls and messages. Apps also allow you to shut off certain functions at different times. For example, disabling text messaging on dinner times.
- Set limits when your child can use a smartphone and for how long each day.
- Set a personal example for your child. Don't bring your phone to the dinner table, and don't text and drive.
- Set up a charging station in a central location in your home. Phones should stay out of your child's bedroom so they won't be in use late at night.

- You can install an app to monitor your child's texting. [Keepers](#) is one type of app that alerts parents about harmful, abusive, or suspicious messages, and it includes a tracking device to show your kid's location in real time. This is especially important, as 19% of youth report having received a sexually-explicit text message.

Smartphone Rules for Your Kids



Tell a parent if someone is making you uncomfortable online



Think before you send. If you wouldn't say it in person, don't send it.



Ask before downloading a new app



Don't post your number online or give it to strangers



Don't answer a call or text from an unknown number



Follow school rules about smartphones in class/on campus



Find opportunities to set an example of proper mobile usage

Implement smartphone rules with your child. Making sure your kids involve you on their phone activities with help keep them safe.

2. Streaming content and smart TVs




Streaming content has shot up in popularity, and there are more TV shows and movies available at our fingertips than ever before – much of it not particularly appropriate for kids. While there are great educational shows on Netflix, Hulu, Disney+, Apple TV+, BBC iPlayer, and others, **children will always be drawn to popular shows** everybody's talking about – without knowing **how violent, sexual or disturbing they could be** for a kid. And there are a lot of opportunities: According to 2019 JAMA pediatrics research performed in the UK, Children aged four to six consume 89 minutes of television every day on average. How can you make sure your kid won't be exposed to unwanted content?



Most of the big streaming content providers have parental controls, some more robust than others. Netflix allows you to set up separate profiles for you and for your children.

Using these tools, you can **ensure that your kids only have access to age-appropriate content**. Because Netflix's children's menu features a different color scheme than the regular menu, you can easily see whether your kids are accessing the content permitted to them or not. However, this doesn't stop kids from moving over to your profile, so you still have to be vigilant.

Monitoring TV Time

How much time should your kid spend in front of a screen?

 60 minutes	 90 minutes	 120 minutes
Preschool	Elementary school	Middle School

-  **Talk to the Kids About What they Watch**
And make sure it's age appropriate.
-  **Use the Parental Controls**
Streaming services will allow you restrict and monitor access for kids.

Monitor TV time by limiting the number of hours they watch per day, incorporating parental settings, talking to your child about the content they watch, and spending TV time as a family.

iTunes and Apple TV allow parents to set rating levels for the content their children watch. By contrast, Amazon Prime features no parental controls, so the only thing to do is to logout of your account and not share the password.

All of these tools, however, do not replace having frequent conversations with your children about what they watch. They need to know that even if a show's name is mentioned all the time, it doesn't mean it's right for them.

3. Gaming consoles and online games

21% of all video game players in the US are under the age of 18. With so many games featuring violent or sexual content, and so many platforms to play on, **it is important to be careful about the kinds of games your children play.**

In addition, many games that have a multiplayer component, or are just entirely based online, which makes them **open to abuse from other players, harassment, and sexual advances** through the game's chat system. Kids may also form relationships with other players and may give away their personal information.

But not all is bad: Games are also a great way for kids to develop a variety of skills. They help children develop problem-solving skills, learn how to commit to long-term goals, and how to work as part of a team. They can also be a great opportunity for family bonding. In order to make sure our kids will enjoy the benefits of gaming and not suffer from its risks, we need to **monitor their gameplay.**

Safe & Secure Gaming

 <p>Know what kinds of games your kids are playing.</p>	 <p>Set their profile to private & choose a fun username.</p>	 <p>Understand the games' ratings and suggested age range.</p>
 <p>Monitor their in-game interactions with others.</p>	 <p>Adjust the parental controls & privacy settings accordingly.</p>	 <p>Keep an ear and eye open for changes in speech and behavior.</p>

Encourage your children to discuss the games they play. Make sure your child profile is set to private. Consider keeping the gaming console in a shared, social space. Study the age rating of the games. Use parental controls to set up profiles. Limit the type of people your child can speak to online.

4. Social media

Social media usage is now ubiquitous among US teens; 71% use more than one social platform. Children nowadays also spend an enormous amount of time on social media. A survey by the non-profit group Common Sense Media showed that **8 to 12 year-olds were online six hours per day**, much of it on social platforms, and **13 to 18 year-olds a whopping nine hours!**

According to a recent Harvard study, even though most social media platforms require users to be 13 years of age to sign up, 68% of parents surveyed had helped younger children set up an account.

Social media can be particularly addictive for tweens and teens. It opens the door to a variety of different issues, like cyberbullying, inappropriate sharing, and advances from sexual predators (more on those below).

Access to social media is also central to teens' developing social identity. It's the way that they connect to their friends, and it can be a healthy way to hang out. The key is to set boundaries so that it remains a positive experience.

Safety Tips for Social Media

1

Discuss the pressure of sharing

Talk to your kids about the value of privacy and making their own choices.

2

Tell them to think before they post

Removing something on social media doesn't mean it's gone forever.

3

Talk about stranger danger

Predators use the social media to track and contact children of all ages. It's important to know who they're talking to and/or adding as a friend.

Create a Safe Environment



Allow your child access only to age appropriate platforms



Monitor your kid's time spent browsing and chatting



Block location access on all social media apps



Adjust settings to make their account as private as possible

Enforce a safe environment. Do not let your kids on social media until they're old enough. Keep the computer in a public location. Limit the amount of time spent on social media. Block location access to all apps. Adjust the privacy settings. Monitor your child's online activity.

5. Cyberbullying

Our children's lives have moved online. Unfortunately, their bullies have moved online, too. Cyberbullying is frequently in the news, with reports of **child suicides due to online harassment**. Cyberbullying starts at younger ages and could have disastrous effects on your child, ones that will require psychological and psychiatric treatments. Young cyberbullying victims are 1.9 times more likely to commit suicide than those who do not experience online bullying.

Cyberbullying occurs across all of the platforms we have outlined above, and it comes in many forms: spreading rumors and sending threatening messages via social media, texting, pretending to be another child and posting embarrassing material under their name, forwarding private photos without consent, and generally posting online about another child with the intent to humiliate them.

Cyberbullying is particularly harmful because it is so public. In the past, if a kid was bullied on the playground, perhaps a few of his peers saw. Now, a child's most private information can be splashed across the internet and is there permanently unless reported and taken down.

Cyberbullying can negatively affect the online reputation not only of the victim, but also of the perpetrator, and have a deep impact on that child's future, including college admissions and employment.

It is also extremely persistent. If a child is the target of traditional bullying, his or her home is more often than not a place of refuge. Because digital platforms are constantly available, victims of cyberbullying struggle to find any relief.

It's often very difficult to tell if your child is being bullied online. It happens digitally, so parents and teachers are less likely to overhear or notice it. **Fewer than half of the children bullied online tell their parents or another adult what they are going through**, according to internet safety organization i-SAFE. In fact, according to the Cyberbullying Research Center, **36.4% of children aged 12 to 18 have experienced cyberbullying in their lifetime.**

The best way to prevent cyberbullying or to stop it in its tracks is to be aware of your child's behavior. A number of warning signs may present themselves.

A child who is bullied may shut down their social media account and open a new one. He or she may begin to avoid social situations, even if they enjoyed being social in the past. Victims (and perpetrators) of cyberbullying often hide their screen or device when other people come into their vicinity and become cagey about what they do online. They may become emotionally distressed or withdrawn.

Cyberbullying

36.4%

of teens report being bullied online

14.75%

of teens admit to cyber bullying others

What to do if your child is bullied online

- #### 1. Document

Take screenshots and recordings of the bullying - it will be essential to expose and stop it.
- #### 2. Report

Inform the school and report the incident to the platform/website. Contact the police concerning threats of violence.
- #### 3. Educate

Make sure the school has a dedicated response in place for dealing with cyberbullying.
- #### 4. Reach Out

Discuss the incident with other parents; maybe more kids were victimized.

How to talk to your kid about cyberbullying



Clarify that liking or sharing hurtful content is unacceptable.



Educate your child about the repercussions of bullying.



Encourage them to reach out to others who are bullied & lend support

Talk to your child about cyberbullying.

6. Privacy and information security

As parents, we are most concerned about the effect of the online world on our children's emotional and physical well-being. It's easy to forget that children are susceptible to information security threats that can cause significant financial harm.

Threats such as **malware and viruses, phishing scams, and identity theft** can have a much better chance of hitting a child – being so much more trusting and less experienced than us adults. To kids, sharing their personal details, such as their full name or where they live, may not seem like such a big deal. **They may even be tricked by a malicious third party into sharing your own credit card details.**

There are a number of ways that hackers and thieves can get information out of children. Free downloadable games, movies, or even ringtones that market themselves to children can place viruses onto your computer and steal your information.

Hackers posing as legitimate companies, like Google, send emails asking for your child's password. They may also pose as one of your children's friends or even a relative.

What should you communicate to your child?

- **Have a discussion with your kids about the big threats online today.** Make sure they know what a phishing attack and a disreputable games website looks like, so they know not to fall for these scams. Also, emphasize the impact that a virtual cyber attack will have in the real world.
- Make sure they **keep all of their information private** and that they never publish their full name, phone number, address, or school they attend in a public place.
- Talk to your kids about passwords. **Having a strong password** is the first and best measure to prevent hacking and identity theft. Using a **secure password generator** like the one we created is great for this occasion, and trying out passwords together is a fun way of ensuring your child's password is as strong as possible.
- Tell your kids to **avoid using public wifi** – this is an easy way for hackers to get into their devices.
- Talk to your kids about identity theft: once a cybercriminal has their data, they can do things in their name and even hurt people – and it will be extremely hard to stop.

What you can do to create a safe environment:

- Install a strong antivirus program on your home computer and the devices of all family members.
- Install a VPN (**virtual private network**) on your computer. This is a software that encrypts your connection and anonymizes your web browsing. It will make it far harder for hackers to access and steal any private information.

- If you and your kids use a lot of different devices around the house, consider [installing a VPN on your router](#). That way, all internet traffic that goes through the router will be protected, without having to install the VPN on every device.
- Install an [ad blocker](#) so your children won't have to face deceptive advertising that encourages them to download malicious programs onto your computer.
- If your kids have smartphones, make sure that their [security settings](#) are set to maximum.

Cybersecurity For Kids



Show them examples of what risky sites/apps look like



Tell them to avoid public WiFi - it's easy access for hackers



Ensure they keep all of their personal info (full name, address, school) private



Teach them how to create a secure password they'll remember

Create a Safe Environment



Get an Antivirus



Use an Adblocker



Limit App Permissions



Install a VPN

Teach your kids the importance of keeping their information and devices safe and secure when going online.

7. Viewing inappropriate content online

Because the internet is so open and public, it is also a place where kids can stumble upon content intended for adults – content which they may find upsetting, confusing or distressing. “Inappropriate content” can mean many things to many different people, from swearing to violence to sexual nature. Also, our kids might be exposed to political or religious ideas we don’t see fit for them.

It’s not easy, but eventually, every parent will need to have a conversation with his children about what they might see online. **Many children don’t go to their parents when they see something they perhaps shouldn’t have seen**, for fear that their parents will be angry at them, and take away their devices or internet access.

If your child comes to you with this type of issue, **the best thing to do is to respond calmly and be open to discussion**. If the content under discussion is sexual, your child will likely be embarrassed already, particularly when talking to their parents about these kinds of issues. Let them know you are there for them and are ready to answer any questions without judgment.

Young people may see sexual content online for all kinds of reasons. They may have seen it by mistake, a friend might have sent it to them, or they may have sought it out themselves out of natural curiosity.

It helps a great deal to talk to your kids honestly and frankly about sex, and a discussion about online pornography is a crucial part. A lot of research has shown that pornography can have a detrimental effect on young people, giving them distorted and unhealthy notions about sex. Pornography can also lead people to think of others as objects, rather than people with thoughts and feelings. At the same time, it’s totally normal to be curious about sex and relationships. **This conversation is a great opportunity to direct your kids to positive resources about sexuality**.

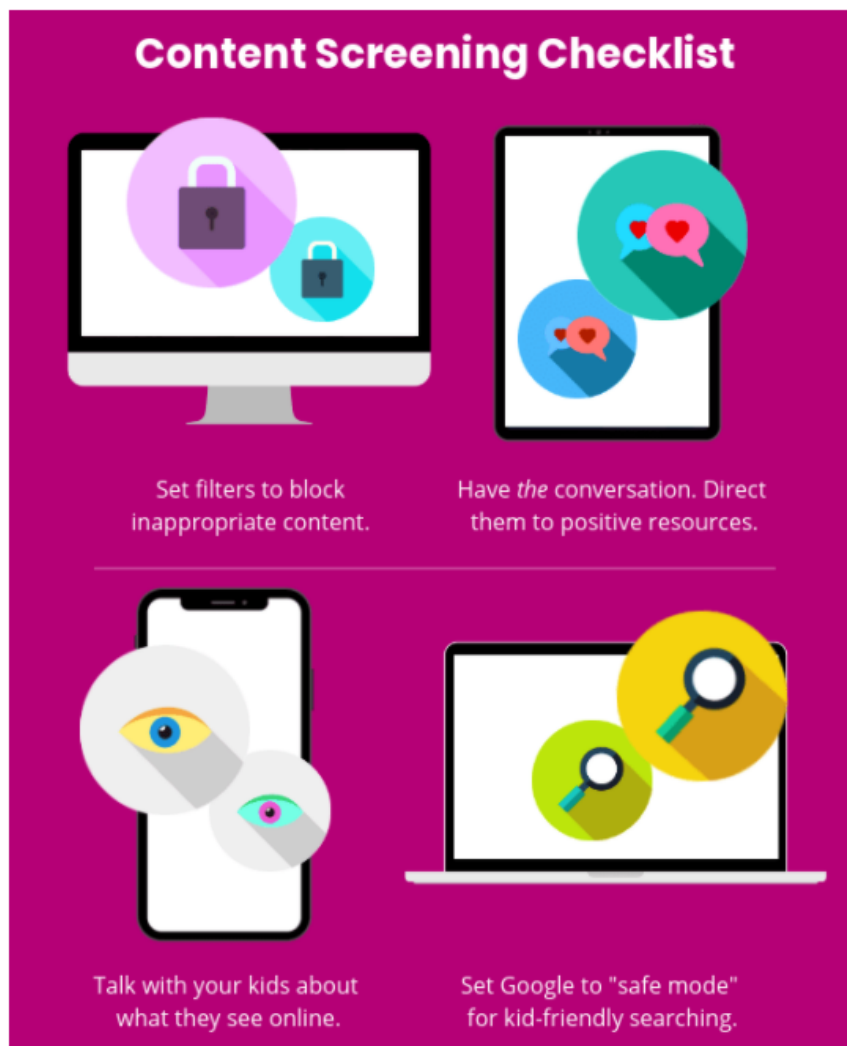
There are also a number of steps you can take to try to prevent your kids from being exposed to content they’re not ready for, like setting up parental controls on your internet connection. Remember, though, that technical fixes can’t replace open communication with your child.

Communicate with your child:

- Let your kids know that they can always come to you if something is bothering them, or if they have questions about anything they have seen online.
- Let them know that it's totally normal to be curious about sex. Direct them to positive online resources like [Brook](#) and [Thinkuknow](#). Thinkuknow is particularly good for younger children, and it includes different, age-appropriate sites for different age groups. You may find it helpful to look through the site together and discuss some of the issues.

Steps you can take to block inappropriate content:

- **Set filters to block inappropriate content like pornography.** Your ISP (internet service provider) should provide free parental controls, as should most gaming consoles. These are usually pretty easy to set up.
- Set Google to "safe mode," so that your children won't inadvertently see inappropriate content in search results.
- Install an [ad blocker](#) to prevent viruses that might have inappropriate content.
- Make sure your streaming services have active child protection profiles, so your kids won't stumble upon rough content while browsing Netflix for cartoons.



8. Online predators

In our last section, we take a look at the darkest and scariest online threat of all: online child predators. According to the US Department of Justice, 13% of young people with internet access have been the victims of unwanted sexual advances, and one in 25 children have been solicited for offline contact; 50% of online victims of sexual exploitation are between 12 and 15 years old.

Predators engage in a practice called 'grooming.' In other words, they attempt to form a relationship with a child with the intention of later abusing them.

The internet has made life a lot easier for child predators. **Predators target their victims through any and all online mediums: social media, email, text messages, and more.**

Predators often create multiple online identities, posing as children to trick kids into talking to them. They discover as much as they can about the children they are targeting by researching their social media profiles – Facebook, TikTok, Snapchat, and others.

They may contact a number of children at once, but tend to concentrate their efforts on the most vulnerable. These predators aren't satisfied with merely chatting with children online. **They frequently trick or coerce their victims into online sexual activity via webcam or by sending sexual images.** They may also attempt to meet and abuse their victims in person.

It's not always easy to tell if a child is being groomed, particularly because most keep it a secret from their parents. **There are a number of warning signs:** children who are being groomed by predators may become very secretive because the predator often threatens the child not to share information with their parents or friends. Children can also become sad and withdrawn, distracted, and have abrupt mood swings. It is absolutely crucial to let your child know that you are there for them and that they can talk to you about anything.



13% of kids with internet access are victims of sexual advances.

Explain to your child:

- Predators are out to get you, so don't talk to strangers online.
- They will try to learn more about you. Keep your address and school private.
- Even nice people can be dangerous. Tell me if a stranger contacts you.

If you think your child is at risk, seek support from their school, a social worker, and the police.



What should you communicate to your child?

- **Have a discussion with your child about the risks of online predators.** Make sure they know to be careful about who they talk to online, and not to share any personal information with strangers.
- Tell your kids that they can come to you with any problem, no matter what it is.
- Think about working through some educational content with your children relating to this topic, like the excellent videos at [Thinkuknow](#).
- If you think that your child is at risk, **seek support from their school, a social worker, and the police.**

Conclusion

There are lots of different technical tools available out there to help keep your kids safe online. These vary from VPNs and antivirus software to internet filters and parental controls. **But none of these are really enough to help keep your child safe.**

As we've repeated over and over in this guide, the key isn't mastering a set of complicated technical tools. (In fact, most are very easy to set up, so don't let a lack of technical ability hold you back). It also doesn't mean you have to master the latest internet fad every time one pops up – believe us, you will never keep up!

The far more important, but also far more difficult task, is to have **frequent, open and honest discussions with your children about their lives.** Remember, internet companies, social media networks, gaming providers, and everyone else in the online space may be able to help you set content limits, but they don't necessarily have your child's best interests at heart.

The very best person to keep your child safe online is you. Talking about how to stay safe on the internet is an excellent conduit to build a trusting and positive relationship with your child.

Internet safety needs to be a priority for every parent and caregiver. If you have found this guide useful, consider sharing it with friends and family via Facebook and Twitter.

Source: <https://www.vpnmentor.com/blog/the-ultimate-parent-guide-for-child-internet/>