

THIRD EDITION

PARENTING IN THE DIGITAL WORLD

A STEP-BY-STEP GUIDE TO INTERNET SAFETY



CLAYTON CRANFORD

PARENTING IN THE DIGITAL WORLD

A STEP-BY-STEP GUIDE TO INTERNET SAFETY

THIRD EDITION

Author Clayton Cranford, M.A.

Copyright Information

Cyber Safety Cop is a registered Trademark 2015 and a product of Total Safety Solutions LLC.

Parenting in the Digital World Copyright © 2015 by Total Safety Solutions LLC. All rights reserved. No part of this book may be reproduced or copied in any manner without prior written permission of the author, except for brief quotations in reviews.

Use of Materials

Readers are encouraged to use the ideas from this book and other Cyber Safety Cop educational materials in their personal and professional lives. We ask that readers give proper acknowledgement to Cyber Safety Cop when they use any examples, ideas, stories, language, or practices that they learned from our program and let others know how to reach our organization—without giving the impression they are authorized or certified by our organization unless they truly are. For any questions about acknowledgement or use, please e-mail info@cybersafetycop.com.

Disclaimer

Products and company names mentioned herein may be trademarks of their respective owners and organizations.

This book expresses the views and opinions of the author. The author will not be held responsible or liable for any damages caused or alleged to be caused either directly or indirectly by this book. The content within the book is provided without warranties. The views and opinions expressed in this book by the author are in no way representative of the author's current or previous employers.

ISBN: 9798723702820

Imprint: Independently published

Dedication

The Cyber Safety Cop program, my work fighting human trafficking, and this book would simply not be possible without the love, patience, generosity, and help from my family. This book is dedicated to them:

To my best friend and loving wife, Gretchen, who has provided me constant support and doses of common sense when I've needed it. To my two boys, Clay and Zachary, who have endured being my cyber safety guinea pigs. I am so proud to be your father.

Finally, this book is dedicated to the parents, teachers, principals, law enforcement officers and counselors who dedicate themselves to keeping our children safe. You do something most people are not willing to do or just can't do. You go the extra mile every day. That makes you special. Thank you.



Contents

Preface	1
Introduction	3
The Cyber Safety Cop Plan	5
When Should I Give My Child a Phone or Social Media?	7
The Problem with Social Media	9
Online Reputation & Privacy	11
Screen Time	14
Online Sexual Exploitation	21
Sexting	27
How to Talk to Your Child About Pornography	32
Bullying	36
Online Threats	42
Identity Theft and Hacking	44
Internet & Mobile Device Usage Contract	46
Create Accountability	49
Popular Apps & Games	52
iPhone & iPad Parental Controls	83
How Children are Hacking iOS Screen Time	88
Android Parental Controls	91
Xbox Parental Controls	99
PlayStation 4 & 5 Parental Controls	104
Nintendo Switch Parental Controls	107
Windows 10 Parental Controls	110
macOS Parental Controls	113
Chromebook Parental Controls	118
Block Porn & Unsafe Websites	122
Parent Monitoring & Notification App	124
Parent Presentation	125
Student Presentations	126
References	128
About the Author	134

Clayton Cranford's book, *Parenting in the Digital World*, is changing lives and helping build safer online families.

What parents, educators, and safety officials are saying about Parenting in the Digital World...

"This was very important. Especially now at quarantine, all kids and teenagers are spending too much time online. This is so scary for all parents because unfortunately this can damage this generation."

Joana J., Hight School Educator

"Unbelievable what information can do for you as a parent. Read this book. It's a great way to be prepared. Social media now has a handbook."

Karla S., Parent

"Being uneducated is not an option. Our children need us. We need to normalize these conversations and continue to pursue knowledge of the new apps that continue to come. The battle for our children's lives is a very, very real thing. This book gave me the words to do that!"

Liset C, Advocate, Human Trafficking Advocacy Program

"Great information for any parent, legal guardian, teacher, social worker and anyone who works with kids to know about how dangerous social media really is and everything you can do for a child who wants to be on social media platforms."

Michelle R., Social Worker Case Manager

"Exactly what I have been looking for as a parent. Clear advice on how to deal with the ongoing issue of social media and kids."

Nathalie E., Parent

"This is a real eye-opener for parents. It gives illustrations of what to watch out for, highlights the consequences of activities, and provides solutions to help create positive outcomes."

Dave H., Parent

"This is an important book because it can help parents and young adults make better decisions, and prevent them from being harmed."

Barbara P., Deputy Probation Officer

"As a father of a child of survivor of Human Sex Trafficking, which started from social media, this book is not only great for professionals who deal with this, but for parents to know how to prevent their children from becoming a victims of bullying, exploitation, or just online drama."

Robert H., EMS Professional and parent of a Human Trafficking Survivor

Preface



Thank you for purchasing the third edition to my book, *Parenting in the Digital World*. It has been four years since I published the second edition, and since that time there have been many new developments in technology. There are new devices, new operating systems, but at the same time a lot has not changed. Parents, educators, and law enforcement are still inundated with incidents of online sexual exploitation, threats, harassment, bullying, self-harm, and suicide. In addition to new apps and devices included in this second edition, I will help guide you through critical discussions every parent must have with their child about pornography and threatening behavior. Technology is a moving target, and we must always be aware of the new and evolving challenges our children are facing.

Speaking with an elementary school principal after I finished a Cyber Safety Workshop for her 150 5th graders, she remarked how important this education is for her students, and how disappointed she was at the lackluster turnout for the parent workshop I did the prior week.

“Every parent of every child in your class should have been there last week,” she exclaimed.

We only had about 25 parents show up to the well-publicized workshop. This kind of turnout is not unusual. If, by sheer coincidence, there had been a cyberbullying incident at the school just before my workshop, we would have had a packed room. The parents who do attend the workshop are blown away by what I show them and insist we schedule another workshop the next month so they can get the word out. They can think of ten parents who needed to be at my seminar. The second class is always better attended. Parents are tired and overworked. I should know. I am a parent of two teenaged boys. After investigating thousands of cyber-related crimes and other incidents, I have gained a perspective that most parents do not have: An unfiltered, unsupervised internet is one of the most dangerous places for our children to be. Why aren't parents attending a free class that will help make the Internet and social media a safer place for their children? After talking to thousands of parents who have attended my seminar, I have discovered many parents are living under false assumptions about their child's digital world.

The purpose of *Parenting in the Digital World* is to bring you up to speed about the potential threats your children may face when they connect to the Internet and abolish the three primary false assumptions parents have about their child's online safety.

False Assumption #1

It is not that big of a deal. The National Crime Prevention Council reported that more than 80 percent of students surveyed said they either do not have set boundaries from their parents about what they can do online, or know how to get around restrictions easily. Nearly 100 percent of parents I talk to after I learned about an issue with their child's online activity had no idea what was going on in their child's online world. They gave their teen or tween a smart phone with no parental controls or restrictions. They are flabbergasted to find their child had created multiple social media accounts, was a victim or perpetrator of cyberbullying, viewing pornography, interacting with adult strangers, or had

sent nude images of themselves to others. There is too much at stake not to be engaged in our children's digital world.

False Assumption #2

If my child was having a problem online, they would tell me. In a report from the Cyber Bullying Research Center (2016), only 1 in 10 children will tell a parent if they are the victim of cyber abuse. Why does only 1 in 10 teens feel comfortable enough to tell their parents about being a victim of cyberbullying? The answer is simple: They are afraid of losing their phone or access to their social networks. Teens would rather suffer through being bullied than lose their vital connection to all their friends. How can we turn that statistic around? We need to make children feel safe to come to us and tell us about problems they encounter online.

False Assumption #3

This technology thing is too much for me; I'll never understand it. Parents are busy working, getting their kids to and from sporting events, and putting a hot meal on the table. The thought of having to take on one more task, as daunting as learning how to operate their child's electronics, makes them want to throw their hands in the air and surrender. The bad news: If you care about your child's safety, you must learn a thing or two about your child's electronic devices. The good news: I wrote this book, *Parenting in the Digital World*, for you. You don't have time to read 200 plus pages about bullying research or scour the Internet on how to set up parental controls on your child's numerous devices. I have done it for you. Even if you know nothing about computers or mobile devices, this book will walk you step-by-step through each of your child's mobile devices, computers, and game consoles, and show you how to turn on the obscure parental controls that will help keep your child safe.

If you are reading this book, then I don't have to convince you that there are online threats and your child is vulnerable. You want to know how to talk to your child about your concerns and understand how all their technology works. You have taken the first step. It may seem scary, but it is worth it. This book will help you the rest of the way.

Introduction



On a bright, sunny first day of school, I walked through the front doors of my middle school and was immediately greeted by the office manager.

“Deputy Cranford, thank goodness you are here!”

Those words and their urgency were not what I wanted to hear walking through the door of my new job as a School Resource Officer. I found Jessica, a 7th grade student, sitting in the counseling office, doubled over in a chair weeping uncontrollably. The school guidance counselor, with a look of sadness and concern, sat next to her rubbing her back, trying to calm the distraught twelve-year-old girl.

Through the tears, Jessica told me that over the summer her boyfriend had asked her to send him a nude picture of herself, which is known among students as “sexting.” She didn’t want to do it, but he pestered her relentlessly until she did. After recounting her story, she framed her torso by placing one hand below her chin, and the other at her waistline and said, “I sent him this.”

Jessica and the boy she sent the image to were no longer “dating.” She believed that he had sent the image to at least one other boy, his close friend. After hours of investigation and interviewing Jessica’s ex-boyfriend and his friend, I was able to delete the image from his phone. He promised he had not sent the image to anyone. His friend had seen the image, but it had not been sent to him by text or email.

What could I tell Jessica and her mother? I could not guarantee that the image was truly gone. The sad truth of the matter was once Jessica sent that nude image of herself to her boyfriend, it was completely out of her control. Her boyfriend could have sent that image to one friend, or fifty. Only time would tell.

What advice could I give them? “Don’t do that again,” wasn’t going to cut it. There had to be more. There had to be a way for Jessica’s mother to supervise her daughter’s online activities adequately, and for Jessica to learn how to navigate cyber space safely.

That experience and hundreds thereafter formed the Cyber Safety Cop program. I created the Cyber Safety Cop program to teach parents and students how to be safe online with all forms of social media.

The goal of this book and the Cyber Safety Cop Workshops are one in the same: Parents will gain an understanding of how important social media and social networking are to their children. They will understand the unique threats that exist online, including cyberbullying, impersonation, identity theft, sexting, sexual predators, human trafficking, digital reputation management, pornography, and other high-risk behaviors.

Most importantly, parents will be given tools and resources to help them properly supervise their children online. They will walk away with a strategy that include: guidelines to be implemented in their home that will immediately make their children more cyber safe.

Students will learn about privacy and why controlling who has access to their social networks is key to a safe and enjoyable experience online. They will, maybe for the first time, come to understand what their digital reputation is and why establishing a good, or bad one, can have lifelong consequences. Finally, they will learn how to deal with bullies and other negative behavior when it inevitably comes their way.

I promise you what I promise every parent or student who attends one of my Cyber Safety Cop Workshops: You will put down this book empowered.

The threats are real and sometimes disquieting, as thousands of teens like Jessica can attest, but by the end of this book, you will have a plan. And something else really special will happen too. You will have amazing conversations with your child about something that is intimately important to them—technology and social media. You will have a window into your child's world. You will see things in your child's social network that will give you amazing insight into what is important to them. Some of it may cause pause, and some of it will affirm what you already know. Either way, it will help you draw closer to your child.



The Cyber Safety Cop Plan

Technology is a moving target. It feels like as soon as you get one new device or social media app figured out, they throw something completely new at us. As a parent, I understand how overwhelming keeping up with our children's technology can be. When I give parents advice on how they should be engaging in their children's digital world, I try to keep it simple, straight forward, and actionable. I don't want parents to throw their hands in the air in frustration and say, "I can't do this!" You can do it, and frankly, there is too much at stake not to do it.

The plan I am laying out for you is based on more than seventeen years of law enforcement experience as a School Resource Officer, juvenile investigator, and behavioral threat assessment expert, and the best current research on the effects of screen time, social media, and pornography on adolescent brains. Finally, this plan is based on more than eighteen years of parenting two boys, who are still wondering what they did to end up with the Cyber Safety Cop as their dad.

1. Educate Yourself

The first step of the Cyber Safety Cop Plan is to become knowledgeable about common online threats and their solutions. This book will cover the main issues such as sexting, bullying, predators, and pornography.

Take the next step by going to a Parenting in the Digital World seminar. You can find a seminar near you on our website's event page, www.cybersafetycop.com. When you are at our website, subscribe to our e-newsletter. It will keep you informed when new apps or threats emerge or just some helpful parenting advice. You will also find helpful articles and downloadable content there too.

2. Talk with and Educate Your Child

Study after study confirms one important fact, the number one safety factor in a child's life is a parent who talks to them. This book will provide you with tools to have an impactful conversation with your child about cyber safety.

Your child's cyber safety education is a critical piece of the Cyber Safety Cop Plan. We created Go Learn Together, an online digital citizenship program for you and your child. Go Learn Together's online lessons will walk your child through critical cyber safety skills. Every lesson concludes with a conversation about the lesson's main between the parent and their child. Try a free lesson at: www.golearntogether.com.

3. Use Parental Controls and Content Filtering

The Internet is vast and there is no end to content that is not appropriate for children's eyes. Your child doesn't need to be looking for trouble to find it online. An innocuous search can land a very young child

on an incredibly harmful pornographic website. Privacy settings on social media platforms will keep unwanted strangers from viewing our children's personal information or from privately messaging. Follow the directions in this book to activate the safety settings in your operating systems, search engines, and games. Setting up content filtering on your home network is a must. This can be done through your Internet Service Provider, Wi-Fi router, or through a service like www.OpenDNS.com.

4. Accountability

When I became a sergeant in my law enforcement agency, my captain gave me an important saying that served me well supervising forty-plus deputies, "You get the behavior you *inspect*, not the behavior you *expect*." If you are not looking for the behavior you want out of your child's digital world, and your child knows you are not looking, you may not get the behavior you want. This requires proactive strategies to stay informed about what is going on in your child's digital world.

First, you should know all of your child's user names and passwords to all of their accounts (social media, email, etc.). Log into your child's accounts as them to monitor activity. Merely "following" them on their social media will not allow you to see areas like private or direct messaging. I also suggest you install a parental monitoring app on your child's mobile devices. We recommend Bark. It actively monitors your child's various online social interactions and alerts you if it sees something problematic. Use promo code "cybersafetycop" at checkout to get 15% off your subscription at www.Bark.us

5. Create Balance

Studies are showing us that the longer children spend on screens the worse they feel about themselves. Teens self-report feeling more lonely, having fewer meaningful friendships, and being more likely to think about hurting themselves.

The Cyber Safety Cop Plan will help you manage your child's screen time by establishing practical limits for school nights and for weekends, and plan family time without electronics.

Implementing the Plan

If you are a parent of a child who does not yet have a phone or social media, you can set up and introduce the plan in its entirety to your child when you give them their phone or first social media account. If your child already has a phone and social media and you are trying to gain some control over their digital world, you may want to implement this plan in bite-sized pieces. An all-at-once program could be such a shock to the system that your child may push back so hard that it could cause significant conflict in your home. There may be situations when the parent has to take drastic action, but if it is possible, the parent should attempt to get their child's buy-in and compliance whenever possible.

When Should I Give My Child a Phone or Social Media?



After a recent parent talk I performed at a large elementary school, a grief-stricken parent walked up to me and said, “I think I made a horrible mistake, I promised to buy my 9-year-old an iPhone for Christmas.” This parent just sat through my two-hour seminar and now realizes what is potentially in store for her daughter and what she, as her mother, will have to do to keep her safe. When a parent asks me when they should buy a phone for their kid, I ask, “Why does your child need a phone?” Are they a pre-teen? Do you drop them off at school/sports events and pick them up? If that is the case, why do they need a phone? Or, how about this: Do they need a smartphone? What about giving them a “flip” phone with no Internet access? Just some ideas to consider. I am noticing an alarming trend at the schools I visit. Younger and younger children are getting phones and social media accounts. Just in 2018, I started performing cyber safety assemblies for kindergarten to third-graders. This is too early for children to have a phone, let alone a social media account. In the screen time chapter, I will go into why giving young children screens too early will negatively impact their mental health and brain development.

The other common question I receive from parents is, “Should I let my [fill in the age]-year-old have [fill in the social media site]?” This is also one of the most common problems that I run into when investigating cyberbullying or an online threat—the child or bully was given a phone or social media too early. Early on in my cyber-threat investigations, I was shocked to find the majority of my cases involved elementary students. In fact, these 10 to 12-year-olds were engaging in this activity more often than their middle and high school counterparts combined. Often, both the perpetrator and victim had parental permission to have their social media accounts or had created the accounts themselves without their parents knowledge.

Every social media site has a minimum age requirement in their user agreement. I have indicated the minimum age for each application along with Popular Apps, and whether they are safe for children.

Facebook and Instagram’s User Agreements state you must be at least thirteen-years-old to have an account. Even Facebook and Instagram think your ten-year-old child is too young. I would challenge parents to ask themselves: Is even thirteen old enough for my child to be on those sites?

There are two good reasons why a parent should never give their child social media before the User Agreement allows, and perhaps even wait a bit longer.

Setting Standards and Not Sending the Wrong Message

When my oldest child, little Clay, was twelve years old, he asked me, “Can I have Instagram?” I replied, “Clay, what’s the minimum age for Instagram?” He replied, “Thirteen.” All children know it is thirteen. I said, “If the minimum age is thirteen, and you are twelve, then the answer is no.” Predictably, his response was, “Dad, everyone in my class has it!” Since this wasn’t the first time I’ve heard that before, I was prepared. “Clay, we are not making our decision to have Instagram based on what everyone is doing, and if those kids lived in our home they wouldn’t have it either.” I went on, “Clay, when you open

the Instagram app for the first time, it requires you to agree to the User Agreement and are at least thirteen years old.’ Clay, if we click yes, are we lying?” When little Clay realized where I was going with this, he looked visibly defeated. He answered in a less than enthusiastic, “Yes.” In our home we talk about truth telling, character, and integrity. Little Clay realized we weren’t going to compromise our integrity to get Instagram a year early, just because everyone else has it.

If we allow a child to have social media before the minimum age, we are telling our children rules don't matter, even the small ones. We are missing out on an important parenting moment.

The Teen Brain is Not Built for Making Good Decisions

This will not come as a surprise to parents, young people make poor choices. Science has finally explained why. Dr. Jay Giedd at the National Institute of Mental Health in Bethesda, Maryland scanned the brains of 145 normal healthy children at two-year intervals. Giedd found that an area of the brain called the prefrontal cortex appears to be growing before and through puberty and doesn’t mature until into a person’s mid-twenties.¹ The prefrontal cortex sits just behind the forehead and is responsible for rational thought and decision-making. As the prefrontal cortex matures, teenagers can reason better, develop more control over impulses and make better judgments.² Research has also discovered that decision making during the teen years, while the prefrontal cortex is still developing, shifts to the limbic system of the brain. The limbic system of the brain is involved in instinctive “gut” reactions, including “fight or flight” responses. These studies suggest that while adults can use rational decision-making processes to navigate through emotional decisions, adolescent brains do not yet have the hardware to think through things in the same way.³ For example, a classmate at school sends a mocking post making fun of Jimmy’s shoes on Instagram for hundreds of fellow students to see and comment on. An adult looks at this situation and easily dismisses it as childhood nonsense. However, Jimmy’s immature prefrontal cortex may not be able to deal with this situation coolly. His emotional feelings of embarrassment may win out, resulting in Jimmy’s decision to lash out on Instagram. The conclusion and implication should be clear: We are giving children who lack the ability to make good decisions the opportunity to destroy their reputations on a permanent medium — the Internet.

Next Steps

- Before purchasing a phone for your child, ask yourself: What are the situations where my child would need a phone?
- What is your child’s school policy about bringing a phone to school or use of a phone during school hours?
- For younger children, consider a “flip phone” with no internet access.
- Before you provide a phone to your child, make sure parental controls are activated.
- Consider installing a parental notification and monitoring app on your child’s phone.
- Review the Mobile Device and Usage Contract with your child before they begin using their phone.



social media access literally at their fingertips. Our social media connected teen is sharing intimate details with potentially 3.5 billion people on the Internet.¹ An unsupervised, unfiltered Internet will leave a child open and vulnerable to threats and attacks that the parent and child are completely unprepared for.

Problem #3

Children believe their digital world and their real-world are two different worlds because they feel different.

This statement seems obvious at first glance, but it's actually more complicated than it looks. It is the key to understanding why children make such poor choices online when they may be moral, level-headed kids in real life. I educate tens of thousands of students every year in school auditoriums across the United States. My main goal is for students to realize that their digital world and the real world are the same world.

When I have investigated cyberbullying or online threats, I interview students who sent a message they later regretted. I always ask them, "Would you say this to their (the victim's) face?" Every one of them says the same thing, "No, I wouldn't have." So, why is this happening? It's simple. Looking at a screen feels different than looking at someone face-to-face. Every student group I have presented to admits this is true. If we all know this is true, then we must start acting differently. Confronting students with this truth will help them begin the process of choosing to behave differently online. Threatening someone to their face is a crime. Threatening them online is the same crime. As parents and educators, we need to engage children to convince them their digital world and their real world are the same because they have the same consequences.

Next Steps

- Take an inventory of all the electronic items in your home or child's life and how they connect to the Internet (e.g., Wi-Fi, hardline, cellular, or a combination)?
- Do your child's devices have parental controls?
- Can your child communicate with another person with this device? How do they communicate (e.g. Text, camera, or voice)?
- Are the people they communicate with a defined group of people that you know, (i.e. private server for Minecraft for just friends), or strangers?
- Can you filter or block the device's ability to communicate with others? For example, some games allow you to turn the chat feature off, or you can unplug the microphone to disable the voice-over-IP chat?

Online Reputation & Privacy



Teens share everything. They want everyone to know how they feel about life, a new song, their science homework, pictures of themselves, where they'll be hanging out with friends, or possibly when they are doing something inappropriate. Parents need to be aware of what their children are sharing in their social networks, how it affects their digital reputation, and the long-term consequences.

When parents give a child access to social media, they should help that child create a positive digital reputation. The added benefit of doing this is finding a positive outlet for your child's creativity, community service, or entrepreneurial interests.

Keys to Shaping a Positive Digital Reputation

Be selective of what you publish online. You should only publish information you are completely comfortable with others seeing. I tell students: before you hit the send button, ask yourself, "If I put this post or image on the side of a bus and drove it around the city with my name on it, would I be embarrassed?" If the answer is yes, then do not send it. Look for opportunities to publish information that will lead to a reputation that will make you and your parents proud. Stay away from using words, symbols, or images of violence, guns and weapons of any kind, alcohol, drugs, pornographic or suggestive material, inappropriate language, and derogatory or racist comments.

It is permanent

Once you publish something on the Internet, it does not belong to you anymore. It can be copied, reposted elsewhere, and used for some unintended purpose. It is true, you can delete posts on social media sites, but often before this can be done, others have screenshot your post, and saved it on their device to be posted later.

Privacy is an illusion

A private post or message is never truly private. Social media apps that claim to delete your content after the recipient reads it (e.g., Snapchat) are easily circumvented. I have personally investigated many incidents where the sender believed a communication was private and later learned the message had been shared with others.

Manage your digital reputation

Periodically perform online searches of your name and nickname and see what comes up. Don't just use one search engine, but a variety of them. If you find unflattering photos of yourself, delete them, or ask the person who posted them to remove them. Your friends might be tagging you in images and posts that you have nothing to do with. Monitor how other people are using your name.

Privacy

Every social media app or platform should have a "Privacy Setting." A privacy setting allows the user to decide who gets to read the text, images, or video they publish in their network. Many social networks like Facebook or Instagram have two privacy choices: Private or Public. A privacy setting is like the

front door to your home. If your social network is set to "Private," then your door is closed and locked. Someone who wants to come into your home has to knock on your front door. You look out through the peephole and decide whether you want to let them in. If it looks like someone you know or someone you can trust, you open the door to them. If it is someone you don't know, the door remains shut. If your privacy setting is set to Public or open, then your front door is left wide open with an invitation for anyone to enter.

Your child should not have a follower that they, or you, do not know (i.e., they and their followers should have a real life, face-to-face relationship). Clear communication with your child is fundamental to helping them make the right decisions online. Use the following points of discussion to educate your child while making your expectations about their online privacy clear.

Use Social Media for Good

A student's online reputation matters. Good or bad, it can have lasting effects on their future. A 2016 survey by Kaplan Test Prep of 400 college admissions officers showed forty percent say they try to learn more about candidates by looking at their online profiles on social networking sites. Thirty-seven percent of the admissions officers discovered something negative.²

According to the career advice website "The Muse," Seventy-nine percent of job recruiters say they will look at a candidate's presence online before making a decision. Seventy percent say they've rejected a candidate after seeing something negative online.³

I talk to students and parents all over the United States about cyber safety and digital reputation management. When you ask a student for examples of how you can hurt your digital reputation, they can give many examples, some from personal experience. When I ask them for suggestions on how they can improve their digital reputation, I am met with blank stares and uncomfortable silence. Across the board, students have no idea how to build a good digital reputation, and their parents aren't much help.

Here is one way a parent can help their child develop a good digital reputation, and it is really easy.

Step 1. Help your child identify a cause or charity they are or can be passionate about. Then look for an organization that supports that cause and posts updates on social media. Have your child "follow" one of the charity's social media feeds (Facebook, Instagram, Twitter, etc).

Step 2. Have your child share (re-post) the charity's posts on their social network. They can include a personal comment about how they feel about what the charity is doing.

Step 3. Encourage your child to find ways to support the charity in other ways. If it's a local charity, go and volunteer with them, or help fundraise in your neighborhood.

Step 4. When your child's friends show an interest in their cause, invite them to help spread the news and volunteer.

I tell students in my workshop, this will do three things:

One, you will look good to anyone on your network and future colleges or business recruiters.

Two, you will be good. Volunteering and serving others has an amazing effect on who you are as a person. You become less self-absorbed and begin thinking about others first.

Three, you will help others be better. The beneficiary of the charity (e.g., homeless people from a food bank, or rescued animals in a shelter, etc.) benefits when you volunteer your time. And when you recruit your friends to help, you are multiplying your efforts. It's a win – win – win, situation.

Screen Time



The internet and social media are amazing technological advancements. We have the ability to know more about the world and other points of view than ever before. Social media platforms like Instagram and Snapchat have become an integral part of many people's lives. Many young people, often called Digital Natives, have never known a world without constant connectivity to the internet and each other. While this presents great opportunities for learning and creativity, a growing body of evidence is raising concerns about the potential implications for our young people's psycho/social health.

Teens spend up to nine hours a day on social platforms,¹ while 30% of all time spent online is now devoted to social interaction.² And the majority of that time is spent on a mobile device. Social media addiction is thought to affect around 5% of young people,³ with social media being described as more addictive than cigarettes and alcohol.⁴

According to a new report by the UK's Royal Society for Public Health (RSPH), an independent charity focused on health education, a growing body of research suggests social media is contributing to mental health problems, such as anxiety, depression, sleep deprivation, and body-image issues in young people. The report combined previously published research on the impact of social media with its own survey of nearly 1,500 people between the ages of 14-24. The survey asked respondents how different social networks—Instagram, Facebook, Snapchat, YouTube, and Twitter—affected their health, both positively and negatively. The survey asked about their feelings of anxiety, connection to a community, sense of identity, sleep, body image, and more. The respondents said that the social media networks they spent the most time on, Instagram and Snapchat, made them feel less secure, more anxious, and less happy about who they are and how they look. However, some social media, like YouTube, was more closely associated with creativity and positive self-expression.

As parents, we need to understand the issues our children are facing in their digital world, and how to engage them in ways that will promote a safe and healthy lifestyle. As we will see, the answer comes down to "balance." We all know that the internet and social media are not going anywhere. In fact, we can expect new technologies (e.g., Amazon's personal assistant, Alexa) to introduce new avenues of social media into our lives in ways we have not considered. Achieving balance is where parents struggle. After spending years working with families as a juvenile investigator, investigating thousands of cases of cyber related issues, I have come to the conclusion that an unfiltered, unsupervised internet is one of the most dangerous places for a child to be. We are also learning that unfettered access to this medium has long lasting mental health implications. Once we understand how social media is impacting our children's mental health, we will look at strategies that will help bring balance back to their lives. Now that children have consistently been on mobile screens since 2010, the data is beginning to show us that unfettered screen time has undeniable negative effects on children.

Impaired Brain Development

A 2019 study published in the Journal of American Medical Association scanned the brains of children 3 to 5 years old (47 brain healthy children – 27 girls and 20 boys) and found those who used screens

more than the recommended one hour a day without parental involvement had lower levels of development in the brain's white matter – an area key to the development of language, literacy and cognitive skills.⁵

You have probably heard of the brain's gray matter. Gray matter contains the majority of the brain cells telling the body what to do. White matter is made up of fibers, typically distributed into bundles called tracts, which form connections between brain cells and the rest of the nervous system. The white matter is responsible for organizing communication between the various parts of the brain's gray matter.

A lack of development of those “cables” can slow the brain's processing speed; on the other hand, studies show that reading, juggling or learning and practicing a musical instrument improves the organization and structure of the brain's white matter.

The MRI results showed that children who used more than the American Academy of Pediatrics (AAP) recommended amount of screen time (an hour a day without parental interaction) had more disorganized, underdeveloped white matter throughout the brain.

“The average screen time in these kids was a little over two hours a day. The range was anywhere from about an hour to a little over five hours,” said lead author Dr. John Hutton, a pediatrician and clinical researcher at Cincinnati Children's Hospital. In addition, the tracts of white matter responsible for executive functions were also disorganized and underdeveloped.

“These are tracks that we know are involved with language and literacy,” Hutton said, “And these were the ones relatively underdeveloped in these kids with more screen time. So the imaging findings lined up pretty perfectly with the behavioral cognitive testing finding.”

Anxiety and depression

One in six young people will experience an anxiety disorder at some point in their lives, and identified rates of anxiety and depression in young people have increased by 70% over the past 25 years.⁶ Research suggests that young people who are heavy users of social media - spending more than two hours per day on social networking sites such as Facebook, Twitter or Instagram - are more likely to report poor mental health, including psychological distress (symptoms of anxiety and depression).⁷ The unrealistic expectations set by social media may leave young people with feelings of self-consciousness, low self-esteem and the pursuit of perfectionism which can manifest as anxiety disorders.⁸ Use of social media, particularly operating multiple social media accounts simultaneously, has also been shown to be linked with symptoms of social anxiety.⁹

Sleep

The connection between sleep and mental health has been known by the medical community for a very long time. Poor mental health can lead to poor sleep, and poor sleep can lead to poor mental health.¹⁰ Ask any parent of a newborn. The necessity of quality sleep is essential for everyone but is critical for teens and their brain development.¹¹ The brain is not fully developed until a person is in their late twenties, and during adolescence, the brain is in a process of furious cognitive development.¹² A growing number of studies have shown that increased social media use has a significant association

with poor sleep quality in young people.¹³ Staring at an illuminated screen, like on phones, laptops, and tablets, right before bed is also linked with poor quality sleep. The exposure of LED lights before sleep can interfere with and block natural processes in the brain that trigger feelings of sleepiness, as well as the release of the sleep hormone, melatonin. This means it takes longer to fall asleep, and individuals end up getting fewer hours of sleep every night.¹⁴ The lack of sleep and emotional investment in social media have also resulted in exasperating feelings of anxiety, depression, and lower self-esteem.¹⁵

Body image

Body image perception is a real concern for both male and female young people, especially female teens and young adults. Sadly, nine in 10 teenage girls say they are unhappy with their body.¹⁶ With 200 million active monthly users on Instagram, who are uploading 60 million new pictures daily, young people have seemingly endless opportunities to be drawn into appearance-based comparisons with others online.¹⁷ One study also found that after spending time on Facebook, girls expressed a heightened desire to change the appearance of their face, hair and/or skin.¹⁸

A 2016 study found strong cross-cultural evidence linking social media use to body image concerns, self-objectification, unhealthy drive for thinness, and general dissatisfaction with current body composition.¹⁹ Plastic surgeon associations have reported a rise in younger individuals opting to have cosmetic surgery to look better in photos. Around 70% of 18-24 year olds would consider having cosmetic surgery.²⁰ A teen's self-comparison to a photo in a celebrity magazine, and comparison to an image on a friend's Instagram are fundamentally different in a very important way. When a young people compare themselves to celebrities, it feels like an apples-to-oranges comparison. After all, the teen thinks, this is a celebrity; they are different from me, and achieving that look or status is a kind of fantasy. But when that same teen looks at a peer's Instagram or Snapchat image, it feels like an apples-to-apples comparison. They are left wondering, "Why can't I be that thin, or why can't I have that much fun?" Consequently, their self-esteem and the perception of their body image suffers, even leading to depression.²¹ To counter these dangerous effects, parents must help their children find a healthy balance for their on-line activities.

The plan to bring back balance in your home

1. Set Priorities

When your child gets home from school, set priorities on the tasks they need to get done. This may include homework, instrument practice, and possibly chores. These tasks must be completed first before turning on entertainment screens (i.e., TV, Xbox, looking at Instagram, etc.). If you have a child who needs breaks during homework sessions (I have that kid), then look for a physical activity to fill that space. Research has shown that physical movement stimulates the brain. I hung a playground swing inside my garage. My son will jump on the swing for a few minutes, and then return to his homework. Sometimes, your child's homework will take them up to their bedtime. This should not mean they get to stay up for an extra hour to get in some screen time before bed. That brings us to setting limits.

2. Set Limits

Setting limits on screen time maybe the most difficult thing parents have to contend with. Screen time is defined as time spent using digital media for entertainment purposes. Other uses of media, such as

online homework, don't count as screen time.

Based on personal experience, and from the common stories of thousands of parents I have spoken to, the earlier you lay down these guidelines, the easier of a time you will have. If you are trying to impose a screen time limit on a teenager after years of unlimited access to screens, expect some push back. You will be shocked to see and hear the irrational reaction from a child when you simply turn off the screens. You may be wondering if that is a sign of addiction. The latest edition of the Diagnostic and Statistical Manual of Mental Disorders (DSM-V) actually includes internet addiction as a disorder that needs further study and research. However, if your child has an emotional meltdown because you limited screen access, don't panic. I would say this is the normal reaction of a young person who spends an unhealthy amount of time online, which frankly, includes most children. If you see an escalation of behavior that does not subside after a day or two, I would suggest contacting your pediatrician to ask their opinion on whether your child needs a psychiatric referral. In a publication of the National Center for Biotechnology Information website, a study conducted by the Department of Adult Psychiatry in the Poland Medical University, showed that Internet addiction was seen to be quite common among young people, especially in children. In fact, every fourth child is addicted to the Internet. This is an alarming statistic that needs to be addressed as soon as possible.²²

How much screen time is too much? Today, in a world surrounded by digital media 24/7, defining screen time is difficult. The American Academy of Pediatrics (AAP) had once set a general screen time limit: no more than two hours in front of the TV for kids over age 2. In 2016, the AAP released new, updated screen time guidelines for parents in the, "Children and Adolescents and Digital Media Technical Report." Dr. Yolanda Reid Chassiakos, lead author of the report, said, "It doesn't make sense to make a blanket statement [of two hours] of screen time anymore... For some children, two hours may be too much." The academy recommends that for children 2 to 5 years of age, screen time should be limited to one hour per day. For kids ages 6 and older, parents can determine the restrictions for time spent using screen, as well as monitor the types of digital media their children use. Babies are most vulnerable to screens. The Academy says that infants aged 18 months and younger should not be exposed to any digital media.²³

My experience working with thousands of teens and their parents suggests that two hours is usually a sufficient amount of entertainment screen time. I highly recommend that screen time should end about 30 minutes to an hour before bedtime. There is a lot of research that indicates looking at a bright screen right before bed will interfere with a good night's sleep. In a recently published study by Tim Smith from Birkbeck University of London, babies and toddlers who spent more time with a touchscreen device slept less at night. On average, each hour that a child spent on a smartphone or tablet resulted in 26 minutes less nighttime sleep, and about 10 minutes more daytime sleep, amounting to 15.6 minutes less total sleep. Touchscreen use was also linked to an increase in the time it took these kids to fall asleep.²⁴

For iPhones, use Apple's Screen Time Limits in the settings (we show how to do that later in this book) or a third-party app for the Android phone. This will help limit screen time by allowing a parent to lock a child's phone at specific times throughout the day, removing the child's temptation to use it when they are not supposed to, such as during school hours or before bedtime.

3. Family Dinner and Screen Free Zones

Establish and enforce screen free zones in your home. The dinner table is a great place to start. In fact, there is a lot of research to show that a screen free, distraction-free, sit-down family dinner has amazing psychological benefits for your children. Family dinners are a sit-down meal with the entire family with no distractions (e.g., phones, TV, laptops, etc.). A 2014 study, published in the *Journal of the American Medical Association Pediatrics*, asked the question: *Do family dinners have any impact on a child's mental health or likelihood to be cyber bullied?* The study measured five internalizing mental health problems (anxiety, depression, self-harm, suicide ideation, and suicide attempt), two externalizing problems (fighting and vandalism), and four substance use problems (frequent alcohol use, frequent binge drinking, prescription drug misuse, and over-the-counter drug misuse) in a national sample of 26,069 adolescents aged 11 to 15 years old. Frank Elgar, Ph.D., a professor at McGill University in Montreal, Canada, discovered that “More frequent family dinners related to fewer emotional and behavioral problems, greater emotional well-being, more trusting and helpful behaviors towards others and higher life satisfaction.” The researchers found the same positive effects of family meal time on the mental health of the young subjects, regardless of gender, age, and regardless of whether or not they feel they can easily talk to their parents.²⁵

One of the more surprising and encouraging findings of this study was more frequent family dinners translated to even bigger benefits for children. “We were surprised to find such consistent effects on every outcome we studied,” said Elgar. “From having no dinners together to eating together seven nights a week, each additional dinner related to significantly better mental health.” What is going on here? It’s not magic, and it has nothing to do with chewing food. It is really about making time to talk with your children. Dinner is a convenient time, because they get predictably hungry and have to stop to eat. And when they do, it is our opportunity as parents to ask them, “How are you doing...what’s going on with your friends?”²⁶

The shared family time presents teaching opportunities for the parents — a time during which parents can model and educate on a variety of life skills such as coping and resiliency as well as positive health behaviors and nutritional choices. The time together allows adolescents to express concerns and feel valued, all elements that are conducive to good mental health in adolescents.

Some parents tell me they have trouble getting their children to talk at the dinner table. In my home, we have a jar of conversation starters that we bring to the dinner table. Each member of the family draws a question from the jar and leads a discussion based on the fun question printed on their card. Some of the questions are fun like, “What’s the funniest or strangest thing that happened to you today,” or telling, “If you were principal of your school, would you change anything? What?” You can find a treasure trove of family dinner conversation starters online with a simple search of: “family dinner questions.” I recommend going to The Family Dinner Project’s website (www.thefamilydinnerproject.org) to see all the great ideas they have to enhance your family dinner time.

4. Engage More

Sarah, a parent of a thirteen-year-old, sent me an email about her experience when she turned the screens off in her home for the first time. Her son James looked at her, confused, and asked, “What

should I do?" She was shocked at the realization that her son did not know what to do in a world without screens. Sarah told me she was at a loss. She never remembered having to ask her parents what she should do to occupy herself. It was something she just did and was perfectly happy to do it.

It seems our "digital natives" are not as good as filling their non-structured time with other activities as we were at their age. Today's youth rely greatly on electronic devices to entertain them and consume their time. They may need a little help and direction. Obviously, the younger we start with our children doing this, the easier it will be.

As a result, you might find yourself spending more quality time with your teen. I have two boys. The younger likes to be outside, shooting baskets, and riding his scooter around the neighborhood with his friends. My older boy likes to be inside, and if he had his choice, he would watch TV or play the XBOX all day. One takes more effort and engagement than the other. They couldn't be more different, but I have found a common activity we all enjoy. We play fantasy and sci-fi board games. They are a fun, cooperative games that require imagination and strategy, featuring zombies, aliens, superheroes, and soldiers, which are, coincidentally, are the types of characters in the TV and movie genres they most like to watch.

5. Charge your teen's mobile devices in your room at night.

When your children go to bed, take their mobile devices out of their rooms and charge them in your room. Electronic devices in a bedroom after lights out is a distraction from a good night's sleep. Many teens have reported to me that merely having an electronic device in their bedroom, even one they know they should not use, causes anxiety. They know it's there, and they are wondering what is going on. They have a condition known as FOMO: Fear of Missing Out. It is impossible for them to turn off their anxiety producing moment-to-moment fear of missing something their friends are sharing.

Remove the temptation and source of anxiety from their room. I recommend that parents not put TVs, computers, or game consoles in their children's rooms either. I tell parents in my seminars: A bedroom is for quiet contemplation, a good book, and sleep – it should be a place where your child's mind and body can relax and unwind.

6. Use social media as a tool for promoting a charity, social cause, or extracurricular activity.

Teach your child that having a voice is a powerful thing. Use social media to reach and inspire others for good. Have them promote a fundraiser, community service meet-up, club, or sports team they belong to on their social network.

7. Likes should not equal self-esteem.

When a teen posts an image in their social network, they get instant feedback in the form of "Likes" or positive comments. Research has shown us that once the teenage brain has linked a behavior to a reward, it continues to seek the reward again and again. Talk to your child about why they are posting images. Is it to share something they are proud of, or to garner validation from others?

8. Be the person you want your child to be.

Take technology breaks and engage with your child. Board games and other structured time with the family are priceless opportunities. Show your child that you have a life outside of social media. Children

do what we do more than they do what we say.

9. Don't be afraid to be the bad guy.

Make a plan and stick to it. Boundaries are essential for your child's safety and well-being. Don't be surprised when you feel push back from your child after you implement these new rules. Remember that these guidelines will help your child's social skills and personal growth.

Create a Family Media Plan

The following guidelines and resources will help you create a functional and healthy media plan for everyone in your home.

Infants

The AAP recommends that no baby under 18 months old should be exposed to screen media, other than video chatting with friends and family. Babies need to interact with caregivers and their environment and not be placed in front of a screen.

Toddlers

The AAP says toddlers interaction with screen media should only be done with their caregiver. The chief factor in facilitating a toddler's ability to learn from baby videos and interactive touchscreens, studies show, is when parents watch with them and reteach the content. The amount of screen media use should be very limited, less than an hour a day.

Preschoolers

Children from 3 to 5 years old can benefit from quality TV shows, such as "Sesame Street," the AAP says. A well designed show can improve a child's cognitive abilities, help teach words, and impact their social development.

The AAP warns that many educational apps on the market aren't developed with input from developmental specialists and can do more harm than good when they take a child away from playtime with caregivers and other children.

And just like toddlers, preschoolers learn much better from any educational materials when they are co-viewed, and the caregiver interacts with the child about the material.

Six Years and Beyond

The AAP has tools to calculate your child's media time and then establish a family media plan. Visit their website to help structure a plan, www.healthychildren.org/English/media.

Two hours of non-educational screens per day is a good goal. Set a schedule and clearly explain your expectations of when screen time is and is not okay in your home. For instance, screens should be excluded from meal times, especially during a family dinner or family sharing time. When you explain to your child why you want to limit screen time (to them, screen time is the favorite part of their day), tell them the reason behind it. Talk to them about the amazing development and growth that is happening in their brain, and how that development can only happen once. As they get older, the development changes and slows. Their early years are critical for making a strong healthy brain.

Online Sexual Exploitation



In December 2014, the parents of a ten-year-old girl alerted the Cleveland Police Department that sexual predators were contacting their daughter through her iPad.

The iPad was intended for schoolwork, but once social media applications like Snapchat and Skype were installed, the tablet became a portal to a dangerous world. After about a month of unmonitored use, her mother checked the device and was horrified to learn that 16 men had been attempting to manipulate her daughter into sexual situations.

The ten-year-old schoolgirl was first contacted by a man on Snapchat, who, after talking about things a ten-year-old would be interested in, turned the conversation to sex. The number of predators who were contacting their daughter grew in a short span of time. Predators who try to sexually exploit children for the purpose of producing child pornography often share that pornography, or access to the child, with other predators. The predator's methodology was a textbook use of social media to manipulate and exploit this young girl.

The anonymity and the global nature of the Internet make its use by sexual predators a predictable threat, although most parents are unaware of the danger it poses to their children. The pedophiles, in this case, are likely based overseas, making identifying and prosecuting them difficult. Police Detectives from Cleveland Police are working with Snapchat and Skype in the hope of tracking them down.

The young victim told many of the men that she was ten years old, but this only encouraged them to ask for explicit images. One of the predators begged her to disrobe and send him nude images and video. He begged, "Open cam baby ... plzzz I like sex. What's the problem, are you not interested in sex?" Another of the unidentified men offered to transfer money to the ten-year-old, so that she might travel to meet him.¹

Unfortunately, her story is not unique. Every day, children in your community are being targeted, snared, and manipulated by a world of sexual exploitation. They are enticed, and sometimes physically coerced, into selling themselves for sex. It is called human trafficking. It is modern-day slavery, without the chains and shackles of a century ago, It is real and happening right under our noses. A community that says, "We don't have that problem," is a community that is deluding itself. How are these traffickers and pimps gaining access to your children? You don't see them cruising the streets of your neighborhoods. They do not need to. They are being invited into your child's life, into your homes, and into your child's most private and intimate conversations, through the Internet and social media.

Sextortion

A parent recently reached out to me with a horrifying and heartbreaking story about his 8th-grade daughter. It was a story that had been going on for the better part of a year, and he was only now just learning of it. His daughter, Kelly, during her 7th-grade year, sent a topless image to her boyfriend. The relationship ended and the image that she intended for only one person to see was shared with others.

On her last day of 7th grade, Jason, a boy at her school, pinned her against the wall and forcibly grabbed her breasts. Kelly pushed him away. Jason smiled and said, "If you tell anyone, I'll send the naked picture I have of you to everyone!" Kelly was terrified into silence.

I could hear the sadness and strain in the parent's voice. He felt he completely failed his daughter. He noticed a change in Kelly following the attack. He described Kelly as "daddy's little girl." She would hang out with him and his wife, chat with them about school and her friends, but something changed. Now he knows why. The summer after the event, she became withdrawn, avoided him, and spent a lot of time in her room on her phone. He thought she was "going through a phase." He heard teenaged girls sometimes do this and wanted to give her space. Looking back on it now, he realizes her reclusive behavior were warning signs she was in a crisis. Something was very wrong, and he felt horrible he missed it. Kelly was anxious and depressed. She had the daily feeling something terrible was going to happen to her. She was assaulted, violated, and then shamed into silence. It was like a heavy weight was wrapped tightly around her chest and dragging her under the waves. She said it felt hard to breathe sometimes.

Kelly went to a new school for 8th grade. She thought maybe the horrible experience of the 7th grade and Jason was behind her. As she settled into her new classroom, she looked up and saw Jason. There he was, standing in her class in her new school. How could this be? She felt the weight tighten again, pulling her down into a pit of despair. Jason walked up to her desk, bumped it with his hip and sneered. Kelly was transported back to the moment Jason pinned her against the wall three months earlier she was trapped and didn't know what to do.

After weeks of Jason harassing and intimidating Kelly, she finally broke. Kelly went to the school counselor's office in a complete meltdown, and that is when she told her story. The counselor called in Kelly's parents and revealed what Kelly had told her. They were being read into the final chapter of a horrifying story their child was starring in, but the story is far from over.

Kelly's father was overwhelmed, fighting the emotional strain of a hurting child and his feelings of guilt and failure. Failure to help and protect his daughter. "I had no idea what was going on," he told me. That summer, Kelly was texting back and forth with a friend who had witnessed Jason's attack. Kelly was trying to deal with the experience the best she could with her friend. Kelly's phone was off limits to her parents. Kelly's father said he wished he hadn't let her live through this alone. He wished he could have seen her messages on Instagram. I told him he could. I explained how to do this over the phone. I also demonstrate how to do this in my parent seminar.

He and his wife are now fighting for their daughter. I recommended professional counseling for Kelly as well as reporting the incident to the school district and law enforcement. Kelly has loving and engaged parents. I have full confidence they will successfully work through this with their child. Kelly's father told me he and his wife will now be a part of their daughter's digital world.

Sextortion can occur in other ways. It can happen over great distances. A shared intimate image with a stranger can open the possibility of extortion. In a famous 2012 case, Amanda Todd, a 15-year-old Canadian student, impulsively flashed her breasts to a web camera during an anonymous web chat. One of the anonymous viewers captured the image and threatened to send the photo to everyone she

knew on Facebook unless she “went back on the camera and put on a show for him.” She refused, and he followed through with his threat. Police came to her home to inform her that the photo of her breasts was circulating on the Internet. On September 7, 2012, Todd posted a 9-minute YouTube video entitled, “My Story: Struggling, bullying, suicide and self-harm,” which showed her using a series of flashcards to tell of her experiences being bullied.² The video post went viral after her suicide on October 10, 2012.

I show the Amanda Todd video in my parent seminar, “Parenting in the Digital World.” There aren’t a lot of dry eyes in the audience when the video ends. It is heartbreaking. Amanda’s mother is now an advocate and speaks publicly against bullying and sexual exploitation, but she desperately wishes she knew what was going in her child’s digital world. In my parent presentation, I tell parents, “Don’t wait for the phone call. Don’t wait for the bad news. The common denominator for nearly all cases of online abuse is an unfiltered, unsupervised Internet.” The good news is parents can filter and supervise it. You don’t have to be an IT wizard to do it. The vast majority of the online incidents I have investigated over the years could have been handled by a parent IF they knew what was going on before it spun out of control.

Online Predators

In my Cyber Safety Cop Parent Seminar, I ask parents where they believe the safest place for their child is. I always hear the same answer: home. Parents generally fear their children being unsupervised outside of the home. The general concern among parents is the possibility of their child meeting someone the parent doesn’t know – someone dangerous. Although this possibility does exist, the rate of violent crime across the country has dropped significantly in the last twenty years. The chance that a teen will ever come into physical contact with a sexual predator in their neighborhood, let alone be snatched off the street, is very low. When we look again at the picture of a child sitting alone in the safety of his or her room, we see something new. The child sitting on their bed now has a mobile device in with Internet and social media access. Our social media-connected teens are not only exposed to people in their neighborhood, or even the population of the United States, but to roughly 3.5 billion people across the Internet. This translates into tens of millions of sexual predators having access to children in their own homes.

Social media platforms are places where predators can actively stalk children, but there are other websites that are passively waiting for children to stumble onto them. Pornographic website chat rooms or classifieds websites are all places where predators are waiting for the curious child to explore. A young girl, looking to get “discovered” as a model or musical talent, may respond to one of many ads on a classifieds website that claims to be a legitimate talent search. These ads are neither legitimate nor safe and have been the source of minors being sexually assaulted and trafficked into the commercial sex industry. The young girls who go to these parties or talent searches are unwittingly walking into a well-constructed trap. The “agent” or “event promoter” is setting up a situation where these girls are being coerced into having sex with men at these events. The coercion is sped along with alcohol and drugs, lowering inhibitions enough to manipulate their victims into complying with their orders.

These traffickers are not the types of people you might expect. They come in many forms. Many pimps

and traffickers will employ other students, such as your child's peers, as recruiters. They may go so far as to plant a recruiter in the school, one who seems sophisticated and talks about the cooler parties she goes to, parties that turn out to be populated with predators looking for young victims. A young girl is more likely to go to one of these parties if she were invited and accompanied by another female student.

The parents of the ten-year-old Cleveland girl believed that they had taken all sensible steps to protect her. They had turned on some of the iPad's parental settings to filter content. Unfortunately, they did not go far enough. In this chapter, I will outline how online predators are using social media to exploit children and offer some truly sensible safety measures to keep your children safe.

To begin, we must understand who the enemy is and their capabilities. The online predator/pedophile is networked with millions of other like-minded individuals who share their techniques and experiences with each other. They know how to identify the most vulnerable victims and what techniques to use to coerce children into sending nude images or videos. In some cases, an accomplished pedophile can manipulate the child, build a relationship, and have the child voluntarily meet or run away with them.

To keep your child safe from these predators, we need to have a basic understanding of how they operate:

1. Online predators look for children who are emotionally vulnerable or who do not appear to have a stable home life. Parents must be aware that every child is potentially vulnerable, no matter their family composition or socio-economic level. However, there are some risk factors that increase a child's danger. The most vulnerable are children who are dealing with a broken home, runaways, or who are in the Child Welfare System. Children share their thoughts, feelings, likes, and dislikes freely on social media. It does not take the predator long to discover who is having problems at home or with key relationships in their lives.
2. The predator listens and sympathizes with the child. These predators are skillful manipulators, and the children they prey on do not have the maturity or life experience to counter their advances. They tell the child what the child wants to hear, not what they need to hear. When a teen laments about being grounded for a week by a parent, the predator says their parent was wrong or stupid, and they should have the freedom to do what they want. The predator begins building an "us-against-them" relationship that drives a wedge between the child and their parents.
3. The predator intensifies the relationship by seducing the child. The seduction phase of the manipulation is key to the pedophile's success. The predator further grooms the child through attention, flattery, affection, kindness, and even gifts. He will make the child feel special. Initial target selection for this phase is very important. Emotionally vulnerable children are craving love and acceptance. The pedophile knows that a properly manipulated and groomed child will not care that he is older. One of the most dangerous aspects of this is that he makes the relationship seem precious, special, so the child, his victim, helps conceal the relationship from their parents.
4. The predator introduces sex into the conversation. Depending on the progression of the third phase, the introduction of sex into the conversation may occur gradually or rapidly. At that point, he does not have to coerce the child into sending him nude images or meeting him.

Human Trafficking

Human trafficking can often go unnoticed, even by individuals interacting with a victim on a regular basis. Recognizing the “red flags,” or indicators, can help alert parents, school administrators, and staff to a human trafficking situation. The Department of Homeland Security (DHS) has identified warning signs of a teen who is being trafficked.³ Recognizing the signs is the first step in identifying potential victims, but it is important to note that there can be innocent explanations for some of these, and no single indicator is necessarily proof of human trafficking.

Behavior or Physical State:

- Does the child have unexplained absences from school, or has the child demonstrated an inability to attend school on a regular basis?
- Has the child suddenly changed his or her usual attire, behavior, or relationships?
- Does the child suddenly have more (and/or more expensive) material possessions?
- Does the child chronically run away from home?
- Does the child act fearful, anxious, depressed, submissive, tense, or nervous and paranoid?
- Does the child defer to another person to speak for him or her, especially during interactions with authority figures (this may include an adult described by the child as a relative, but may also be a friend or boyfriend/girlfriend)?
- Does the child show signs of physical and/or sexual abuse, physical restraint, confinement, or other serious pain or suffering?
- Has the child been deprived of food, water, sleep, medical care, or other life necessities?
- Is the child in possession of his or her own identification documents (e.g. student identification card, driver’s license, or passport), or does someone else have them?

Social Behavior:

- Does the child have a “boyfriend” or “girlfriend” who is noticeably older?
- Is the child engaging in the uncharacteristically promiscuous behavior, or making references to sexual situations or terminology that are beyond age-specific norms?
- Can the child freely contact friends, family, or his or her legal guardian?

What Should I Do if I Suspect SOMEONE IS Being Trafficked?

From the DHS website: If you suspect that a person may be a victim of human trafficking, please call the Homeland Security Investigations Tip Line at 1-866-347-2423 (24 hours a day, 7 days a week, in over 300 languages and dialects) or submit a tip online at www.ice.gov/tips.

You may also call the National Human Trafficking Resource Center at 1-888-373-7888 to get help or connect with a service provider in your area. The Center is not a law enforcement or immigration

authority and is operated by a non-governmental organization.

Non-law enforcement personnel should never attempt to confront a suspected trafficker or rescue a suspected victim directly. Doing so could put both your and the victim's safety at risk. By immediately informing law enforcement of your suspicions, you can safely assist in the recovery of the victim and the dismantling of the trafficking operation.

School administrators and staff who suspect a trafficking incident should follow their school district's established protocol for such matters. Schools that do not have such procedures in place should consider adopting a formal protocol on how to identify the indicators and report suspected cases to law enforcement. Your protocol should be developed in collaboration with school district leadership; federal and/or local law enforcement; mental health, child welfare, or victim services providers; and other appropriate community partners. (DHS.gov, 2015)

DHS offers free online Human Trafficking Awareness Training at:

<https://www.dhs.gov/blue-campaign/videos/general-awareness>

Sexting



Rachel's finger nervously hovered over the send button. She stared down at the picture she took for Jeremy, her first real boyfriend, debating if she should send it. In the 6th grade, it seemed like all the popular girls were "hooking up" with boys. Rachel was trying to fit in, and Jeremy was so cute. All of her friends said she was lucky to be "going with him." The night after they officially declared they were dating, Jeremy sent a text. "Send me a picture of you [winking face emoji]." Rachel replied, "What kind of picture?" Jeremy said, "In your underwear ... Just for us [heart emoji]." Rachel knew of three other girls who had sent "nudes" to their boyfriends and even boasted about it later. She thought, It's not such a big deal, right? Rachel took off her shirt, stood in front of the mirror, and took a picture just for Jeremy. Her finger hovered over the send button an extra moment until she told herself, don't be such a baby. She pressed her thumb down on the send button, a decision she could never take back.

I was called to the school a week after Rachel had sent her intimate image to Jeremy. The night Jeremy received the picture from Rachel, he forwarded it to three of his friends. Rachel discovered the photo had gotten out when one of Jeremy's friends came up to her after class and asked for a "nude." When Rachel said she wouldn't do anything like that, he said, "I know you do! I saw the picture you sent to Jeremy." Rachel went to the counselor's office sobbing. She felt betrayed and scared.

I interviewed Jeremy and his three friends. The image of Rachel did not go any farther than the four of them. They agreed to delete the photo. I watched them delete the picture from their phones and from the cloud. I hoped there weren't any other copies, but there was no way to be sure. Rachel's parents were beyond stunned. They described their daughter as shy and introverted. "She's not that kind of girl," Rachel's mother told me. I explained to Rachel's parents when a child is looking at a screen and not another person, the inhibitions go away. Rachel is not that "kind of girl" in the real world, but in the digital world, anything is possible. Although the pictures were deleted, the damage to Rachel's reputation was done. Rachel was relentlessly bullied for sexting. Jeremy turned on her and said she got him in trouble when she told the school they were sexting. A month later, Rachel's parents transferred Rachel to a new school.

I wish Rachel's story were unique. It is not. I have sat across the table from too many Rachels and their male equivalents. Boys are just as likely to sext as girls, and they are just as likely to be damaged by it.

What is "Sexting?"

Sexting is the electronic exchange of sexually suggestive or explicit content in messages, photographs, or videos, between at least two people.

To most teens, "sexting" is a normal way to interact with their peers. I have asked thousands of teens in my cyber safety presentations about their perceptions of sexting. The general belief is that "everybody is doing it," especially when you're "going out with" someone. What does the data say? 54% of teens under the age of 18 admit to having sent sexually-suggestive messages or inappropriate pictures.¹ We know that 53% of teens who sext are girls while 47% are boys. 1 in 5 teens has sent or

posted nude or semi-nude pictures or videos of themselves. Almost 20% of teens have reported being forwarded a picture or video that was not intended for them, with over half of those teens admitting to forwarding it on to more than one other person.²

When Should I Talk to My Child About Sexting?

You should talk to your child about sexting and sending other inappropriate images/videos as soon as you give them a phone. Please do not wait until you stumble on something on their phone or for an incident to occur. How you talk to your child about this issue may change based on their age, but this is a conversation that comes with receiving a phone. A young child with no interest in sending a nude could, through no fault of their own, get a request for an explicit image or receive a photo without their permission. No matter their age, they need a plan to deal with the realities of their digital world.

How Do I Talk With My Child About Sexting?

As always, remain calm and don't lecture. When I was on the Hostage Negotiation Team for my police agency, I learned a powerful technique that I used to gain understanding and compliance from those who may not be interested in complying - ask questions and be a good active listener. Your tone should denote a desire to know what your child thinks. It should not sound like a test. By asking questions, not only do you have the opportunity to gain some understanding of your child's perceptions, but you are inviting them to be a part of the solution. Try asking:

- Why do some kids sext? How big of a deal is it?
- Are there safer ways to show someone that you trust and care about them?
- Do you think a photo posted on the internet will remain private and anonymous forever?
- How could that kind of image affect you or your future?

Asking questions and listening is a technique we should be using whenever we are having difficult conversations with our teens. It helps tamp down the emotional volatility that comes with some of these discussions. When you finish your talk with your child, leave an open door. This is not a one-time conversation. As your child matures and starts exploring different relationships, the issue of sexting will come up again. Make sure your child knows that they can come to you anytime they need to talk. You should also realize that you might not be the person they feel most comfortable talking to about this. Consider approaching another trusted adult (e.g., youth pastor, coach, etc.) or a professional counselor to be a sounding board for your child.

Your discussion's ultimate goal is to change the way your child thinks about sexting and to have them consider the long-term consequences of their behavior. One challenge is that your child's decision-making part of their brain, the pre-frontal cortex, which takes long-term consequences into account, has not fully developed. The prefrontal cortex doesn't fully develop until a person's late twenties. While the prefrontal cortex is still developing, teens rely on their brain's impulsive pleasure-seeking center to make decisions. In the emotionally charged moment when a teen chooses to take and send a nude picture, they may not be able to pause and consider the consequences. We know talking to children about making good choices makes a difference, so don't give up.

The following are topics you should cover when you are talking to your teen about sexting.

Sexting Could Be a Crime

Nude or partially nude images of minors can be a crime. They might be considered child pornography. Although state laws vary, in some states exchanging nude photos of minors also is considered a felony—even when the images are taken and shared consensually. 61% of teens don't realize that sexting is considered child pornography.³ They said that if they'd known, it probably would have deterred them from sexting.

A Sent Image Belongs to Everyone

Begin by discussing with your child that you can never get the image back once it is sent. The image is out there forever, and you have no control over what happens to it. Ask your child how they would feel if their friends, teachers, parents, or the entire school saw the picture. When an intimate image is shared with others, the teen in the photo could be bullied, exposed to sexual predators, and at risk for blackmail.

Talk about pressures to send or ask for revealing pictures.

Let your child know there might come a time when someone asks them for an intimate image. Tell them that no matter how significant the social pressure is, the potential social humiliation can be hundreds of times worse. After I had finished teaching a cyber safety assembly at a middle school, a couple of students came up to me to share their own experiences. An 11-year-old female student told me, "A boy in my class texted me one night and asked for a nude. I didn't know what to say, so I laughed and said I had to go. Since then, he has asked me a few more times. I don't know what to say." I replied, "Be direct. Tell him, I respect myself too much to do that, and if you respect me, you won't ask again." She smiled, said "thanks," and ran off to her next class. Helping our children strategize how to deal with these issues is always a good idea.

We need to speak to our children, especially our boys, about asking for intimate pictures from others, even people in dating relationships. The "casual" request is very concerning to me. Where does a boy get the notion that asking a girl for a nude image is ever okay? Where does a girl get the notion that she needs to give a boy an intimate photo of herself to prove she's in a relationship? I believe the prevalence of pornography and its growing normalization in our culture is at the core of this issue. As you learned in my chapter on pornography, nearly a third of middle school boys said they watched porn at least once a month or more, and 29% said online porn was the most useful source of information about sex. What is porn teaching our boys about sex, love, and relationships? Porn teaches them that women are not human beings; they are things. You can do whatever you want to them. That includes things that are painful, humiliating, and even violent. The woman in the video acts as if it's pleasurable, so the boy watching thinks this is how you treat a woman; this is what she wants.

The request for a nude image is nothing more than the attempt to fill an endless desire for new and exciting porn. There is a total lack of respect and empathy in such a request. They are not thinking about what could happen to a person's reputation if that image gets out. We need to start by addressing porn in your child's life. Talk to them about the detrimental effect of watching porn has on their lives and how porn can warp our perception of a healthy relationship. Have frank conversations with your teens about the pressure to ask for and send nude images. Ask questions to gain insight into

your teen's perceptions about sexting. Ask them about the possible dangers and consequences of sending a sexually suggestive message to strangers or someone they know. Once they have a clear understanding of the risks to the sender, ask them if it's safe or fair to ask someone to create an intimate photo and send it to them.

Don't forward inappropriate images.

Your child might get an unsolicited sext sent to them. It is very common for students to receive these accompanied with a message like, "Can you believe this is Jenny?" or "I just got this forwarded to me, did you get it too?" Talk to your teen about this possibility and what they should do if it ever happens to them. If someone sends them a photo, they should delete it immediately. It's better to be part of the solution than the problem. Forwarding images that constitute child pornography is a crime, not to mention the harm it will cause to the photo's subject. The image was likely shared without their permission, and by forwarding it, you are now part of a chain of abuse. Tell your teen it's okay to say no if someone asks them to forward an image. Many people get pressured by their friends, especially boys, to share nude images of their girlfriends or boyfriends. It can be hard to stand up to this pressure. Ask your teen to think about how much giving in could hurt their girlfriend/boyfriend.

Reputation Consequences

I received an email from a recent college graduate who was applying for jobs and internships. She was anxious and hopeful to start the next chapter of her life in a career she was passionate about. She had promising interviews but was receiving rejection emails. She learned that a Google search of her name revealed a website that had a nude photo of her. This was a photo she had given her now ex-boyfriend when they were still dating. She contacted the website and demanded they remove the image. They offered to remove the picture for \$5000. She asked me if law enforcement could help. The website was hosted in another country. United States laws could not help her get the photo removed. She asked if they would remove it if she paid them the ransom. I told her I didn't know. It is possible that they could take her money and then ask for more. She had zero leverage or recourse in this situation. This is a case of revenge porn, which is illegal in several states, but our laws have little influence on foreign entities.

We live in a world where most college scholarship committees and businesses check their applicants' public social media or Google search results. The long term potential risks are real. It is worth considering the likelihood that an image will not remain private.

What to do if you discover your teen is sexting

Remain calm

Remaining calm in this situation may be very difficult. Deep breaths and repeating the mantra, "remain calm," over-and-over in your head may be necessary. Remember, your child has no life experience to help them navigate this issue, and as discussed earlier, the decision-making part of their brain is not fully developed. Fight the urge to punish them immediately. Swift discipline will not help your child in the long run. Remaining calm and talking to your child will help you understand why this happened and what you need to do next.

Talk to them about the situation.

Emotions may be running high, and you may feel incredibly disappointed in your child's decision. Be careful not to shame your child. Sit down with your child and talk about the situation in a calm, gentle way. Start the conversation by admitting that you both are uncomfortable talking about this. Assure them that you do not want to make them feel worse; you just want to understand what happened and how you can help. Ask questions and be ready to listen without making personal judgments. Instead of making accusations or casting blame, seek to understand your teen. After you feel like you have a good understanding of the situation, the next step is to address the images and social media.

Delete any photos or videos.

If your child receives a nude photo, have them delete it right away. If your teen has naked pictures of themselves, have them delete those too. There might be copies of photos on the device's camera roll or in a photo folder. Check to see if those images have been backed up in the cloud. They will need to be deleted there as well. Avoid looking at the photos, especially in front of your child, and don't show them to other parents. I have had many parents tell me that they wish they had never looked at them. Once you understand the severity of the photos, move on to taking action.

Consider working with other involved parents.

If the sexting occurred between two minors, your child and their classmate/boyfriend/girlfriend, consider reaching out to the other child's parents and work together to resolve the situation. Depending on your level of comfort and how well you know the other parents, call them or meet with them to discuss your children and say, "Our teens have been sending and receiving sexual images. I'd like for us to work together and address this."

Consider informing law enforcement or the school.

If you believe that your child is exchanging sexual images with an adult, you should contact your local law enforcement agency and report it. Your child is a victim, even if they voluntarily sent an explicit photo to the adult.

If your child is involved in a sexting-bullying situation at school, it may be useful to have outside intervention through the school and disciplinary action. Some schools have mandatory reporting requirements, which means that they must report this activity to law enforcement. If you decide to work with the school to resolve this issue, it could also mean involving law enforcement matter.

Ultimately, sexting, like many other parenting challenges, comes down to communication. Start the dialogue with your pre-teen early. Help them to see that you are an advocate, that you are on their side, and they are more likely to come to you when they have problems later. Remember that they are facing new and complicated challenges that are as confusing and difficult for them as they are for you. The more you educate yourself about those problems, the better prepared you will be to help them should those situations arise.

How to Talk to Your Child About Pornography



I received an urgent text message from a parent named Sarah through Cyber Safety Cop's Facebook page. Sarah's message read, "My six-year-old was exposed to porn on my iPad. Please help me!" I wish this were a unique or infrequent message; it's not. Too many parents are shocked to learn their very young child has accidentally stumbled onto a pornographic website. It is so easy to do. A very innocent Google search can result in pornographic content. I talked to Sarah for more than an hour on the phone. What came through the phone was an utterly devastated mother. Weeping, she recounted what happened. Two days earlier, she gave her six-year-old son her iPad to keep him occupied while putting away the groceries. She heard him drop the iPad and run away to his room. When she picked up the iPad, she was horrified at what she saw. She found her son hiding in his room. He could not process what he saw, and she didn't know what to say. All she could do was hold him. Over the past two nights, he had not been able to sleep alone in his room. We talked about options for getting him help and how to keep something like that happening again. Sarah said, "I feel like I failed him...I never thought I needed to put parental controls or web filtering on my iPad. I don't look at those websites. It never occurred to me that I needed to put them on for my six-year-old." Like so many other parents that I have spoken to, Sarah is not only mourning the harm to her child but feels responsible. I told her she was in good company with many great parents who have found themselves in the same situation.

The Internet has made hardcore pornography more accessible than ever before. More people visit pornographic sites than Twitter, Netflix and Hulu combined. As the prevalence of pornography grows online and in popular culture, so does nearly forty years of scientific evidence that viewing pornography has catastrophic effects on our lives.

When we talk to our children about cyber safety and appropriate online behavior, we must address the issue of online pornography. Talking to your child about sex is not easy. The mere thought of having to talk about pornography will produce significant levels of anxiety in most parents. Not only are you faced with the uncomfortable task of talking to your child about why they should not view pornography, but you will be fighting the prevailing popular cultural view that pornography is victimless and beneficial. Nothing could be further from the truth. Next to street drugs and alcohol abuse, pornography is becoming one of our society's most serious public health issues.

When we talk to our children about pornography, I don't think it is enough to say, "Just don't watch it." This is not a compelling argument against all the hormones and neural chemicals flooding their brains when they look at porn. When it comes to drugs or porn, discussion with children (especially with boys) must explore the bigger picture. Porn is not neutral. Porn will have hurtful effects on the viewer and others. We need to make a case that will be meaningful when our children leave the shelter of their home router's firewall, and when they are connected to an unfiltered world of pornography.

I have two teenaged boys. I sat down and shared four evidence-based points with them: 1) Porn hurts your brain; 2) Porn hurts women; 3) Porn hurts families, and 4) Porn fuels human trafficking. I will lay out the case for each point and then show how you put it all together when you talk to your children.

Pornography Hurts Your Brain

What do cocaine and online pornography have in common? As it turns out, quite a bit. Deep inside your brain is a thing called the “reward pathway.”¹ The reward pathway is an important mechanism for our survival. It connects behavior to a feeling of wellness or pleasure. It does this by releasing chemicals—mainly one called dopamine, but also others like oxytocin.² These neural chemicals are very powerful, and for a good reason. They promote or reward activities that are essential to life, like eating, sex (procreation), or for accomplishing a difficult task (hunting and gathering).³ These chemicals are what make us feel happy and euphoric. Unfortunately, they can be hijacked by street drugs and pornography.⁴

Street drugs like cocaine and heroin make the user feel high by triggering the reward pathway to release high levels of dopamine. Viewing pornography uses the exact same reward pathway as hard street drugs. Remember, the reward pathway’s purpose is to lead the user back to the behavior that triggered the chemical release. The surge of dopamine through the brain does more than make the user achieve a euphoric high; it helps to create new brain pathways. In other words, it changes their brain. The more a drug user injects heroin or a porn user watches porn, the more those pathways get wired into the brain, making it easier and easier for the person to turn back to using, whether they want to or not.⁵ This is called addiction. If an adolescent is watching porn, these brain changes and neural pathway wiring to porn is happening at a crucial time in their cognitive brain development.

Yes, you can become addicted to watching porn. Porn also has the same trajectory as other substance addictions. Over time, a junkie will eventually require more and more of a drug to get a buzz or even just feel normal. In the same way, porn users can quickly build up a tolerance as their brains adapt to the high levels of dopamine.⁶ In other words, even though porn is still releasing dopamine into the brain, the user can’t feel its effects as much. As a result, many porn users have to find more porn, find it more often, or find a more extreme version—or all three—to generate even more dopamine to feel excited.⁷

Pornography Hurts Women

In almost all porn, women are nothing more than objects used to satisfy the sexual desires of the man. Women in the videos are depicted as being happy with whatever the man wants to do, even if it’s painful or humiliating. A study of the most popular porn videos found that nine scenes out of ten showed women being verbally or physically abused, yet the female victims almost always responded with either pleasure or appeared to be neutral.⁸ As a result, male porn users’ ideas of what sexual or loving relationships should look like are often warped.

In an anonymous survey of 247 Canadian junior high school students whose average age was 14 years, James Check and Kristin Maxwell (1992) report that 87% of the boys and 61% of the girls said they had viewed video-pornography. The average age at first exposure was just under 12 years.

33% of the boys versus only 2% of the girls reported watching pornography once a month or more often. Additionally, 29% of the boys versus 1% of the girls reported that pornography was the source that had provided them with the most useful information about sex (i.e., more than parents, school, friends, etc.). Finally, boys who were frequent consumers of pornography and/or reported learning a lot

from pornography were more likely to say that it is “OK” to hold a girl down and force her to have intercourse.⁹

Pornography Hurts Marriages and Families

Research has found that marriages in which one person has a porn problem or sexual compulsion are often plagued by less intimacy and sensitivity, as well as more anxiety, secrecy, isolation, and dysfunction in the relationship.¹⁰ Studies have found that married porn users are more likely than non-users to have sex with someone other than their spouse.¹¹

When I cover the effects of pornography in my parent seminar, I often see women in my audience dabbing tears from their eyes. They come up to me after the talk and share how their marriage is failing or has failed because their husbands are addicted to online pornography, and now they are trying to protect their sons from it. A spouse’s frequent use of pornography leads to a loss of trust and intimacy. In a survey of members of the American Academy of Matrimonial Lawyers taken in 2002, 62 percent of the divorce attorneys surveyed said that obsession with porn had been a significant factor in divorce cases they had handled in the last year.¹²

Pornography Fuels Human Trafficking

On the nightly news, we often hear horrifying stories of sex trafficking here in the United States and around the world. We are appalled and disgusted by those who would hold women and children against their will for nothing more than objects for sexual pleasure. I volunteer and support Agape International Missions in Cambodia. I have traveled to Cambodia several times and seen firsthand the physical and emotional toll this evil inflicts on the most vulnerable. At the same time, we live in a culture that celebrates pornography as a banner example of the First Amendment. These opposing views of sex trafficking and pornography must be addressed.

There is a connection between “mainstream” pornography sites on the internet and desire of child sex trafficking. The \$100-billion pornography industry is fueling the appetite for children.¹³ Teenage girls now make up the biggest slice of viewable porn. A Google Trends analysis indicates that searches for “Teen Porn” have more than tripled between 2005-2013, and teen porn was the fastest growing genre over this period...[reaching an] estimated 500,000 daily in March 2013, representing approximately one-third of total daily searches for pornographic web sites.”¹⁴

In Melissa Farley’s 2007 article, “Renting an Organ for Ten Minutes:’ What Tricks Tell us about Prostitution, Pornography, and Trafficking,” she interviewed 854 women in prostitution in 9 countries. Almost half (49 percent) of the women she interviewed said they were forced to perform in pornographic films while they were in prostitution.¹⁵

If you are watching pornography, you are supporting a system that is helping enslave men, women, and children all over the world.

Putting it All Together and Having the Talk

I want to give you a strong argument against pornography in your child's life and in your life too. When you talk to your child, explain to them why you choose not to view pornography. Make your reasons for not watching pornography personal. The strongest arguments come from the heart.

This is how I shared with my two teenaged boys:

"I have chosen not to watch pornography for several reasons. I want to share them with you and explain why pornography is destructive, and how, if you let it into your life, it can hurt you and the people you love. My reasons are not my opinion but based on a lot of science and research, which I can show you later if you are interested.

First, I won't watch porn for the same reasons I won't use street drugs like heroin. Viewing pornography can lead to addiction. Science has shown us that the chemicals that get released in the brain when someone does drugs are the same chemicals that get released when they watch porn. Addiction destroys you from the inside out, and that includes your health, your job, your friendships, and your family. I work hard to support you and this family. My ability to do that comes from having a healthy mind and soul. Addiction, of any kind, hurts and enslaves your mind and soul.

Second, pornography hurts women. I respect your mother and all women. Pornography objectifies women. That means, women are seen as nothing more than a physical object, made less than human, and their only value is to sexually satisfy men even when the sex acts are painful or hurt them. That's why boys who watch pornography feel the crime of rape is not as serious than boys who don't watch porn. And, because we respect women, we never ask a girl to send us a nude image of herself.

Third, I don't watch porn because I love you and your mother. Watching porn opens up your mind and heart to the idea of having a relationship with someone other than the person you are married to. I love you and your mother too much to do anything that would hurt you, your mom, or break up this family.

Fourth, I don't watch porn because some of these women who are in these videos are not there because they want to be. Some of them are being forced to do it. I refuse to be a part of a system that enslaves people and steals their dignity. And lastly, many of the women who are on those videos are forced to have sex against their will. They are given drugs or beaten if they don't make those videos. When someone clicks on a porn video, they are hurting another person. If no one were watching pornography, those girls would be free. (Perhaps play "Refuse to Click" video for your child if you think it is appropriate for them).

I have put filters on your devices and on the computer to keep you from purposefully or accidentally watching porn. I know that I can't guarantee that you will not see it somewhere else, like on a friend's device. Just like with drugs, I can't be with you all the time to make sure you make the right decision. Ultimately, it will be up to you. You cannot watch pornography without someone getting hurt.

I want you to be prepared when someone offers to show you pornography of any kind. What do you think would be a good way to say no?"

"No, I don't want to see it because porn hurts women," or

"No, don't send me that image/video, I don't want those images in my mind."

Talking to your child about online pornography is not easy. If we want our children to have healthy perceptions of women and healthy relationships, then we cannot ignore it.

Bullying



Jill's first day of high school was a hopeful one. After two and a half years of torment by the hands of three girls in middle school, Jill was finally free of the daily feeling of dread she had been experiencing. The three girls were her friends when she was in the sixth grade, but the relationship turned sour when Jill was selected to be on the dance team, and the alpha-member of the three was not. Everything changed for Jill on that day. The exclusion during recess and harsh looks didn't end at school. Jill was subjected to ridicule on social media. Her evenings and weekends were filled with anxiety. She would lay in bed at night unable to sleep wondering what were they saying about her now on Instagram.

Jill felt like all that was behind her now. She turned the corner in the hallway to her first class, and there they were. The three girls that had been the source of her torment were standing in the middle of the hall as if they were waiting for her. They burst into laughter when they saw her. Jill could feel her insides melt. There it was, the old feeling of despair had returned. The tightness in her chest threatened to choke her. She pushed past them and winced when she heard "bitch...slut" uttered under their breaths.

I found Jill in the counselor's office, sobbing uncontrollably. All she could say was, "I wish I were dead, I don't want to be here," over and over again. Sadly, Jill's story is not unique.

In a recent study from Rutgers University, girls are more often bullied than boys and are more likely to consider, plan, or attempt suicide.¹

You may be asking, aren't boys bullied? How is this different? Yes, boys are bullied. Bullying among boys is often physical. Schools are cracking down on physical bullying which people can see — making them more preventable by school officials.

Among girls, bullying is often the kind that's not visible. It's often relational bullying, such as excluding someone from activities and social circles or spreading rumors about them. The actions are not overt. This type of bullying can go on for a long time without anyone else knowing, and it does. I have conducted thousands of bullying investigations as a school resource officer, and the teen girl-on-girl bullying is often the worse kind. It's not that it is more violent or extreme than boy-on-boy bullying. It's a grinding down process that can span years.

School should understand the differences in bullying and how we might better address females who are bullied. Parents need to understand the differences too and not look at bullying as a right of passage. Telling your child, "Everyone gets bullied. You have to buck up. Stand up for yourself," will not address the harmful effects bullying is having on our children. Bullying today, with the advent of social media, is fundamentally different than the bullying today's parents faced when they were teens. We need to empower our children against bullying. Here are four ways we can do just that.

1. Model compassionate, respectful relationships from the time your child is small.

As a professional threat assessor, I have learned, victims beget victims. Children who experience the trauma of bullying will often become bullies themselves. As parents, we need to raise our children in loving, respectful relationships, rather than relationships that use power or force to control them. Children learn both sides of every relationship, and they can mimic either one. Disciplining children by yelling and belittling them will teach them that bullying is okay.

2. Teach your child how the dynamics of bullying works.

Research shows that bullies begin with verbal harassment. How the “victim” responds to the first verbal aggression determines whether the bully continues to target this particular child. If the aggression gives the bully what he’s looking for – a feeling of power from successfully pushing the other child’s buttons – the aggression will generally escalate. It’s imperative to discuss this issue with every child BEFORE they might be subject to bullying, so they can stand up for themselves successfully when a bully first “tests” them.

3. Teach your child how to respond to teasing and bullying.

Role play with your child how she can stand up to a bully. Point out to your child that the bully wants to provoke a response that makes the bully feel powerful, so showing emotion and fighting back is exactly what the bully feeds off of. Explain that while your child can’t control the bully, she can always control her own response.

The best strategy is always to maintain one’s own dignity, and to let the “bully” maintain their dignity. In other words, to keep your dignity while withdrawing from the situation, and not to attack or demean the other person. To do this, remember this three-step process:

1. Remain calm. Expect to feel scared or anxious. That’s normal and okay. Take a big breath, or two, before you speak.
2. Disarm by saying: “I’m going to ignore that comment,” or, “No thank you,” and walk away calmly. The instigator will try again at a later time. When they do, repeat step-two.
3. If it doesn’t stop, give the instigator a choice. If after repeating step-two several times, and they are not getting the hint, “take it to the next level.” Say: “I’ve given you several chances. I think you know I am not interested. If this continues, I’ll have to take it to the next level. I don’t want to, but I will,” and then calmly walk away. Your child doesn’t need to explain to the instigator what “the next level is.” If the instigator continues to ask what the next level is, say: “I think you know.” The next level is asking an adult at the school for help. Explain to your child they have given the instigator several chances to stop. If they can’t get the hint, then your child should go to a teacher or school administrator and ask for help mediating the situation.

Cyberbullying

There are many examples of cyberbullying. Sometimes it is as simple as hateful text messages or hurtful posts on someone’s social media account. That type of bullying is closer to what older generations experienced as playground taunts and insults. Such words are certainly hurtful and

harmful, but they are usually private communication between the perpetrator and victim. The internet offers even more harmful, public methods of bullying, which continue to live on the internet indefinitely, coming up in searches about the victim years after the incident took place. Sometimes such bullying involves editing and reposting an unflattering photo or forwarding an embarrassing picture. But sometimes, the perpetrator takes it even farther, as happened in the following example.

On a Sunday evening, Carlie, a 12-year-old 7th grade student at a large middle school, received a text message from her friend Gina. In the text, Gina said someone had created an Instagram account with Carlie's picture on it and was saying "bad things" about her. Carlie went to the Instagram account, and was horrified at what she found. The profile image was a picture of Carlie, taken from her Instagram account. The account name was, "Carliewherebitchslutugly," and the bio read, "I'm a slut bitch, I hate everyone." Within an hour of the fraudulent account's creation, hundreds of Carlie's classmates were already following it and commenting on the images the account's creator had posted. Carlie's eyes began welling up with tears as she scrolled down and read the comments. The person who created the account was posting and commenting as if she was Carlie. The posts were pornographic and horribly malicious. What made the posts incredibly hurtful were the comments from Carlie's classmates, some of whom she considered friends. Her classmates were liking and commenting on the disgusting posts created to devastate Carlie. "LOL," and "LMAO," peppered the hurtful comments. Carlie looked for someone to stand up for her; to say that these posts were gross. She couldn't find one classmate objecting to the beating she was taking online. She felt very alone and scared. Carlie was afraid to tell her mom and dad. She knew that they would "freak out," take her phone away, and call the school. Her phone and her ability to connect with her friends was too important to lose. She was also afraid that if her parents called the school, things would only get worse. Carlie decided to say nothing and go to school the next morning hoping it would blow over. Bullying situations like this one never blow over; they have a life of their own. They blow up.

Four days later, the principal at Carlie's school called me. "Deputy Cranford, we have a bullying situation on Instagram. We need your help." When I arrived, I found Carlie with another girl in the principal's office. Carlie was brought up to the front office because she had been caught in a hair-pulling fight with another girl. When Carlie found out she was being suspended for two days for fighting, she showed the principal the fraudulent Instagram account. It became clear that the stress of dealing with the account had been too much for Carlie, and she'd snapped. The girl Carlie had fought with wasn't the girl who created the account. She was just a classmate that had teased her about the Instagram account.

Finding the culprit was easy. Carlie knew who had created the fraudulent Instagram account. They liked the same boy and had been openly hostile to each other over the past few weeks. I flagged the account as a fraudulent account (I explain how to do this on page 84), which violates Instagram's user agreement, and the account was deleted within the hour. Unfortunately, since the fraudulent account had been online for more than four days, students had already taken screen shots of the posts and shared the screen shot images on their personal accounts. Even though we were successful in removing the offending account, we will never truly remove the posts it generated from the internet.

The phenomenon of bullying is nothing new. Any parent who was bullied as a child can recount that experience with great detail. Cyberbullying does share certain characteristics with traditional

schoolyard bullying, but there are important and distinct differences. As we will see, these distinct differences make cyberbullying in many ways more psychologically hurtful and physically taxing than traditional bullying.

My parent workshop does not include a definition of bullying. The term bullying is chronically overused. It is being used to describe virtually any situation between children that involves mean-spiritedness or hurt feelings. I do not want parents to be distracted with a label. I want them to focus on the behavior. Rude, aggressive, hurtful behavior needs to be addressed whether it occurs once or repeatedly. It is important to have a clear definition of bullying because behavior that qualifies as bullying is different and significant. It is more serious in its effect on the victim and even the bully.

Anyone working in the school system, kindergarten through high school, knows hurtful words and mean-spirited play make up a majority of student-to-student interaction. Is every one of these incidents a bullying incident? If all anti-social behavior is bullying, then practically every child is a perpetrator, and everyone is a victim. In such a broad context, bullying has lost all meaning. Can a one-time hurtful message impact a student to the point of causing significant psychological distress? The answer is, yes. But is it bullying? A good definition might help clear up this question.

Every major child health or anti-bullying organization has published its own definition of bullying. I believe one of the best and most meaningful definitions of bullying is provided by Stopbullying.gov, a federal government website managed by the U.S. Department of Health & Human Services.²

Bullying is unwanted, aggressive behavior among school-aged children that involves a real or perceived power imbalance. The behavior is repeated, or has the potential to be repeated, over time.

Cyberbullying does not neatly fit into the above definition of bullying. It does not require the bully to be bigger or stronger than the victim. The Internet is the great equalizer of power. Everyone has an equal voice; therefore, the imbalance of power is transitory at best. A single comment or image can become viral, growing exponentially. Because of that, a single act can have the same effect as a repeated attack on the victim.

Effects of Cyberbullying

Victims of cyberbullying tell me they feel helpless. Blocking the bully or turning off their phones does not solve their problem. It is like a malevolent force, growing in power, turning their friends against them. The ever-present nature of the Internet and cyberbullying creates a constant low level of stress in the victim. Children caught in this syndrome of cyberbullying-induced stress can have all the symptoms of Post-Traumatic Stress Disorder (PTSD).

It's not just the victim that needs help. After investigating hundreds of cyberbullying incidents, I have learned that the bully needs as much help, maybe, even more, help than the victim. A 2012 study, published in the *Journal of Abnormal Child Psychology*, found that victims of bullying, frequently bullied fellow students themselves.³ It is important to remember that child perpetrators are themselves also victims. For that reason, the goal of the juvenile justice system is not to lock up kids or throw them away. The goal is to intervene, educate, and restore.

How to Respond to a Cyberbullying Incident

I encourage parents to empower their children with the tools necessary to resolve a bullying incident on their own. Of course, this may not be possible in every case, especially when violence is involved. My experience is that most students want the opportunity to resolve their own conflicts with other students. Unfortunately, many parents never give them the opportunity. Parents immediately call the teacher or principal to intervene. The following are steps I recommend to students in dealing with rude or bullying behavior in my Student Workshop:

Step #1: Do not respond and do not retaliate

A natural reaction to an inappropriate message is to hit the reply button and fire back. Unfortunately, if the recipient does that, they are playing into the instigator's hands. As with other types of conflict, whatever moral ground the recipient might have been standing on as the victim quickly erodes away when they retaliate. On many occasions, I have been asked to help unravel complex online bullying situations at school. One student claims he is the victim, while the other says he is the victim. Scrolling back through the text messages, I find a back and forth of insults, hurled from both sides. It is impossible to know which child is the aggressor. In these types of situations, it is not uncommon for both students to face discipline regardless of who started the name calling.

Step #2: Don't be a bystander

It is difficult for victims to ask for help. They are either scared that the harassment will continue or escalate, or that they will be branded a "snitch." In my experience, most of the reports of inappropriate or threatening behavior was made by a third party or "bystander." Engaging students, potential bystanders to report hurtful behavior is a key resource for discovering and intervening in bullying incidents before they escalate. Anonymous or confidential online/text based reporting systems are very helpful in facilitating student reporting. Students need to understand when they report incidents of bullying; they are not getting the instigator in trouble, they are helping them. After investigating hundreds of cyberbullying incidents, I have learned that the bully needs as much help, maybe, even more, help than the victim.

Step #3: Document the abusive behavior

If possible, take a screen shot all of the mean, rude, or threatening messages immediately. If the instigator thinks you are going to report them to the school or police, they may try to cover their tracks by going back and deleting their remarks or their entire account. This is especially critical in the case of a threat of violence. Although law enforcement can sometimes recover deleted messages directly from the social media provider, having a picture of the post or message can help the authorities better know how to proceed.

Step #4: Report abuse to the hosting site

All reputable social media sites have member guidelines and user agreements that prohibit abusive behavior. They also have a mechanism that allows users to report posts, images, or accounts that violate the site's user agreement. The site then has a procedure to review, remove, or ban users who violate those established guidelines. Prompt removal of abusive content is very important and can help mitigate future problems.

Step #5: Block the instigator from contacting the victim

The final step may be the most obvious. Use the options on social media sites and on smart phones to block accounts and phone numbers from allowing the instigator from contacting the intended target. Some students I was worked with have had to completely retreat from social media because of hurtful messages and post from anonymous users. The instigator is looking for a reaction. Often times, with no one willing to play their game, they get bored and move on.

Step #6: Attempt parent-to-parent resolution

If the steps 1 through 5 do not address the inappropriate online behavior, a parent or school official should be contacted. If possible, I encourage parents to attempt to resolve the issue parent-to-parent. Once a parent has gathered the facts and gained a good understanding of what is going on, remember that children make mistakes, and most issues (not including threats of violence or criminal activity) can be handled at the parent level. I encourage parents to reach out to the parents of the student who made the inappropriate post or message and tell them what they learned. An accusatory tone will be met with defensiveness. Remember, the goal is to de-escalate the conflict between students, not winning points, or retaliation. If the communication between parents does not stop the inappropriate behavior, then I advise parents to take it to the next level which includes the school administration and the School Resource Officer.

Online Threats



I have investigated hundreds of online threats at schools. The vast majority of students who made threats were good kids who made a bad choice with no desire of hurting anyone. They were angry or frustrated at another student and said something they could not take back. Today we live in a world of school shootings. Schools and law enforcement take every threat very seriously. Students do not fully appreciate the potential consequences their threatening statements can have. In some cases, those consequences can have life changing effects.

A student I will call “Sean,” found himself in the Principal’s office again for being disruptive in class. The principal explained that since this wasn’t the first time Sean had been sent to his office, Sean would have to be sent home with a one-day suspension. Sean’s mother was at work and gave the principal verbal permission over the phone to let Sean walk home, as he only lived a few blocks from the school. As Sean walked home with a suspension notice in his pocket, he couldn’t think of anything but how his teacher had it out for him, and now he was probably going to get grounded by his mom too.

After reaching an empty home, he took out his smartphone and opened Instagram. Anger and frustration welled up inside of him. He found his teacher’s Instagram account. He grabbed her profile image, posted it on his Instagram feed and impulsively wrote, “THIS IS THE UGLY ASS BITCH THAT GOT ME SUSPENDED!” Without a second thought, Sean hit the send button. One like, two likes...23 likes on that post. Sean wasn’t finished. He continued, “THE FIRE INSIDE ME IS BURNING RN [sic], AND I WANT TO CUT THAT BITCH.” The posts were public. There was no taking them back. The moment Sean hit the send button, he committed a felony.

I was a member of the county-wide school threat assessment team. I responded daily to the 189 schools in my jurisdiction. The school threat assessment team and I were alerted by the school’s principal who sent me several screen shots of the posts. I arrived at Sean’s apartment and sat down with him and his mother. I did a full threat assessment to determine if Sean posed a threat to the school or the teacher. My assessment was that Sean was angry, and at the moment he posted those comments had no intention of hurting his teacher. Sean, like most teens, has impulse control problems and has no sense of accountability when using social media.

I wrote a crime report that in time disappeared from his record after Sean successfully completed the classes and counseling appointments in our diversion program. Unfortunately, the same cannot be said about his school record. His one-day suspension turned into a five-day suspension, and he was finally expelled. At Sean’s expulsion hearing, I was called to give the facts of my investigation. Sean looked at me with tears in his eyes and said, “I am so sorry, I am so sorry.” I replied, “I am sorry too, Sean.” It was too late for me to help him. If Sean applies to a college, he will have to disclose that he was expelled for threatening a staff member with great bodily injury or death. Not too many schools are willing to take on that kind of liability.

Sean’s story is only one of many. I have interviewed more than a hundred students during my tenure

as a threat assessor, and unfortunately many end like Sean's story. Sean was sixteen, and teenagers make mistakes. Sean, like others living in the internet era, are making mistakes on the permanent medium of social media, and often you can't take back those choices.

In my student assembly, I have an open and frank discussion with students about this problem. Every student that I have interviewed for making a threatening remark online always said the same thing, "I didn't know this could happen to me." Their juvenile brains couldn't control their impulsive anger or consider the consequences of their actions. Schools are moving to a zero-tolerance position when it comes to threats. There is little room for error on the part of the student or school.

The Airport Rule

Share my rule with your student: The Airport Rule. All students know this rule when they walk through airport security. I ask the students, "Who here has flown on an airplane?" Every hand goes up. Then I ask, "What is the one thing you cannot say when you are walking through airport security?" Inevitably, a student shouts out, "I have a bomb."

"What happens if you say those words, even if you are not serious?" Again, the students know the right answer: "You will be pulled out of line, miss your flight, have all your bags searched, and be interrogated for several hours."

School is like the airport. If you say guns, bombs, knives, shooting, killing, or any other violent word while in school, you will be pulled out of your class, have all your bags searched, be interrogated by other investigators like me, receive school discipline, and possibly be charged with a crime.

The Airport Rule doesn't just end at school. Your online world is like the airport. If you post images, post comments, or directly message another person about guns, bombs, knives, shooting, killing, or any other violent word, you might end up with a law enforcement officer knocking on your door late at night. Social media provides little to no context to our words. Jokes or violent song lyrics can sometimes be interpreted as a threat. Once a remark online has caused a disruption at the school, the student who made that remark may be subject to school discipline even though the comment was created away from school.

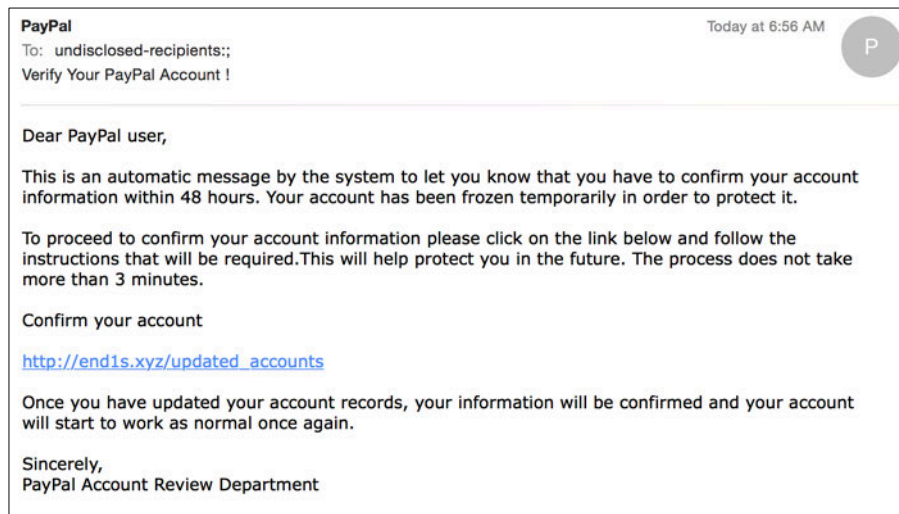


Identity Theft and Hacking

When we give our children an email account, social media, and access to the internet, they become vulnerable to online scams and identity theft. Children and the elderly are a rapidly growing segment of online fraud victims.

If you are like most people, when you think of “cyber attacks,” you imagine hackers using lines and lines of code to launch super-sophisticated attacks against international corporations and governments.¹

The truth is one of the most common forms of cybercrime is actually fairly simple. The majority of accounts, social media or bank accounts, are hacked because the user unwittingly gave the hacker all the information they needed: their username and password. The most common method of doing this is through a phishing (pronounced: "fishing") scam.



The target gets an unsolicited email from what looks like a legitimate source (bank, Facebook, etc). The email may say, "We have found possible fraudulent activity on your bank account. Sign in to verify your purchases." The panicked target will click on the link or button provided in the email. They are taken to a website that also looks legitimate. They enter their username and password and press "enter." The target has just entered their log-in information into a shell site, and their username and password have been sent to the hacker, who is now quickly logging into the target's account and taking their money.

How can we tell if this email is legitimate or not? Have a close look at the PayPal email and then we

will explore the tell-tale signs of a phishing scam.

How to tell if you are the target of a phishing scam:

1. Always regard unsolicited emails that request your personal information with skepticism. It is unusual for a bank or social networking site will email you about fraud. Usually, banks will call you on the telephone. Regardless, close the email and go directly to the website on your browser, or call them with the number printed on your bank statement.
2. Never click on any links or attachments in the email. It is critical that you NEVER click through to a website or open an attachment from an unknown/unsolicited email. Clicking on a link may take you to a fraudulent website, and opening an attachment could launch an application on your computer that will infect your system with a virus or malware. One particularly bad malware going around is "ransom-ware." It is a program that locks up the contents of your computer and can only be unlocked if you pay the people who did it. These people live in Russia or China, making prosecution impossible.
3. Check the destination of the links. If you hover your cursor/pointer over the link in the email (do not click on it), you will see the link's destination. You will see that the destination web address is NOT your bank or Facebook.
4. Read it carefully. Many of these scammers are from foreign countries. English is not their first language. You will commonly see misspelled words or obvious grammar mistakes.

You are now probably asking yourself, what do I do if I get one of these emails? Do I call my local police agency?

If you are a victim of Internet crime, report it to: The Internet Crime Complaint Center (www.ic3.gov). IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Parents, share this information with your child if they have an email or social networking accounts. Your children are easy prey to these phishing scams. Their Instagram account can be taken over by a hacker, ransomed or used for some other nefarious purpose.

Internet & Mobile Device Usage Contract



In a poll reported by the National Crime Prevention Council, more than 80 percent of teens surveyed said they either did not have parental rules about Internet use or found ways around the rules.¹ Cyber Safety Cop wants to turn that statistic around. The number one safety factor in any child's life is a parent who will talk to them and help them develop coping strategies. The Internet & Mobile Device Usage Contract is a tool to help parents start an ongoing conversation with their children about social media and the Internet. The contract does the following:

- Sets boundaries around what behavior is and is not appropriate.
- Sets expectations about what their child should do when encountering inappropriate content or behavior.
- Clearly defines your child's expectation of privacy, which starts at zero and is left to the discretion of the parent.
- Sets reasonable consequences if the child does not abide by the rules of the contract.
- Creates a safe environment which will encourage a child to confide in their parent(s).

How Do I Use the Contract?

The Cyber Safety Cop Internet & Mobile Device Contract is not unlike other Internet contracts you can find online with a casual Google search. What is different about this contract is how you use it.

Sit down with your child and read each line of the contract with them. At the end of each line, follow up with an open-ended question. It will go something like this:

"Number one, I will not give my name, address, telephone number, school name, or parents' names to anyone I meet on the computer. Why do you think that is a good idea? Have you ever seen someone do that before? What could happen if you told a stranger what city you lived in?"

Do this with each point of the contract. When you get to the final point of the contract, tell your child what their consequences will be if they do not follow the rules of the contract. Be reasonable in your discipline. Make sure you can carry out the consequence you threaten. Don't be the parent who does not have a plan, and in distress says, "You are losing your phone forever!" Well, at some point that parent will have to cave in and give the phone back. Not a good precedent to set.

Finally, you want your child to come to you if they see or do something inappropriate online. Only one in ten children will tell their parents about something inappropriate they saw online. If they think they will lose their phone or access to the Internet if they tell you, they may hide what happened and hope you never find out. To encourage your child to be upfront with you, you must include grace in this contract.

Your conversation with your child might go something like this:

“I am giving you a mobile device and social media because I trust you. I also know you will make mistakes, or you will see something inappropriate that you know I would have a problem with. Here’s the deal: If you come to me immediately and tell me what happened, I will help you. I will not punish you. If you forget to tell me or hide it from me, I will punish you.”

Use this Contract as a spring board to begin an ongoing discussion with your child about being safe online.

Download a copy at www.cybersafetycop.com/resources

Internet & Mobile Device Usage Contract

I understand that using the Internet or my mobile device is a privilege, which is subject to the following rules:

1. I will not give my name, address, telephone number, school name, or parents' names to anyone I meet on the computer.
2. I must tell my Mom and/or Dad all of my social networks' usernames and passwords. They have access to all of my files/apps (anything on my device) at any time.
3. I will not download anything or install apps or games without first asking my parent(s).
4. I understand that some people online pretend to be someone else. I will never let someone into my social network that I do not already have a real face-to-face relationship with.
5. I will not fill out any form online that asks me for any information about myself or my family without first asking my parent(s).
6. I will not buy, order anything online, or give out any credit card information without first asking my parent(s).
7. I will never write or post anything online that I would not want my parents to see. I will not use profanity or offensive language.
8. I will promote _____ (a cause or charity) that helps others in my social network as a condition of having a social network.
9. If someone sends me any pictures or any e-mails using bad language, mean rude, or threatening words, I will not respond and tell my parent(s).
10. If someone asks me to do something that I am not supposed to do, I will not respond and tell my parents.
11. I will not call anyone I meet online or in person, unless my parent(s) say it is okay.
12. I will never meet in person anyone I meet online, unless my parent(s) say it is okay.
13. If I receive an inappropriate photo from someone, I will not respond or show my friends. I will immediately tell my parent(s).
14. If anyone I meet online sends me anything in the mail or by email, I will tell my parent(s). I will not keep online secrets from my parent(s).
15. If I make a mistake or see something inappropriate, I will tell my parent(s) as soon as possible.
16. I will respect the house rules for technology and screen time.
17. If I do not follow the above mentioned rules of this contract, I will accept the consequences my parent(s) give me, which may include (but is not limited to) losing access to the internet, my phone, or any other electronic devices.

Signature of child

Date

After signing, post visibly by computer

Signature of parent

Date

Create Accountability



If you have implemented the recommendations in the book so far, you have created boundaries with parental controls and content filters, and established rules and expectations with the mobile device contract. Now comes the most difficult part: Creating accountability. Accountability is the foundation of discipline. Without it we are setting up our children for failure.

Step #1: You own your child's phone

One day, Shellie, a neighborhood friend and mother of two teenaged children, asked me how to open her son's phone. I thought she didn't know how to operate her son's iPhone, so I took my phone out to use as an example and began showing her where the power button was. She stopped me mid-demonstration and said, "No, I know how to turn it on. I don't know his passcode." Surprised, I wasn't sure what to say at first. I said, "Well, you have him tell you what it is, and then you open his phone." She told me she tried, but he would not give it to her. I finally understood her situation. I replied, "Well, that's easy. Take the phone from him, and in an hour or two, you'll find him curled up in a fetal position in the corner of his room. I bet he'll give it to you then." Shellie had abdicated her power and authority over her son's phone, letting him believe his phone belonged to him and that he had an expectation of privacy. When I told Shellie she owned his phone, and had every right legally and morally to invade his privacy, her eyes widened, "Really?" she asked. "Yep, it's yours," I told her. If you have read the chapters on pornography, human trafficking, and cyberbullying, I don't need to convince you of this truth: There is too much at risk for us not to engage our children in their digital world. I often have parents ask me, what do I say to my children when they try to guilt me with not trusting them? I have had this exact talk with my teen. Not only did it give me a chance to talk to him about his online safety, it became a lesson in integrity. This is what I said to him:

"In this home, we don't have secret lives. Your Mom, at any time can pick up my phone and look at everything I am doing. I can do the same to her phone. She knows that when I am not at home, I am honoring her and this entire family with my actions. Because I don't have secrets, I have nothing to fear or hide from. Secrets are what get us hurt and in trouble. If you are embarrassed by something going on in your phone, and you want to keep it secret, then there is a real problem in your life you are not dealing with. I love you too much not to know what is going on in your life."

Step #2: Log into your child's accounts

Know all of your child's usernames and passwords to all their devices and accounts. If you allow your child to have a social media account like Instagram, you should have the Instagram app on your phone, and be logged in as your child. I have two teenaged boys who both have Instagram accounts. I have added their accounts to the Instagram app on my phone. Whenever they get a follow request, or when one of their followers comment on their pictures, I receive the notification as well. Since I am logged in as the account holder, I can view their accounts and see everything going on, including direct messages.

Step #3: Physically check and monitor

Your child is sitting on the couch glued to their phone, fingers tapping away at the screen, giggling at the wittiness of their post, and completely oblivious to what's going on around them. Sound familiar? I encourage parents in this scenario to walk up to their unsuspecting teen and take YOUR phone (remember they don't own anything in your home) out of their hot little hands in mid-text. Your child's reaction to you taking YOUR phone will be very instructive. If they clutch the phone to their chest, sit on it, or run out into the street with it – you have a problem. There should be only one acceptable reaction, the child calmly handing the phone to you. When you have YOUR phone in your hand, standing in front of your bewildered child, take a minute or two and scroll through their text messages or Instagram posts. This is a spot check. You may find something of concern, but mostly you are doing this for a specific effect. You are making the statement: This is my phone, I am monitoring what is going on, and I love you.

Step #4: Install a parent notification app

Monitoring your child's online activity may seem like a full-time job. It isn't easy. I recommend installing a parent notification app on your child's device. There are many to choose from. They vary in cost and features. Here are a couple features you may want to look for when choose the right app for you:

- Provide safe internet browsing
- Reduce/end texting and driving
- Track and locate kids' devices
- Manage screen time limits
- View all app on kid's devices
- Monitor text and browsing activity
- Block in-app purchases
- Block YouTube or other age restricted content



I am a big fan of Bark, a parent notification app that blocks inappropriate websites, monitors texts, email, and social media. It works on both iPhones and Android powered phones. I have a promo-code for you. Enter “cybersafetycop” when you sign up to get 15% off your subscription forever. Bark is available on the Apple App Store, Google Play, and at www.bark.us.

Step #5: Charge devices in a parent's room at night

In the “Create Balance in Your Child's Life” chapter, I explained why having a phone or device in a child's room at night is harmful. When you collect your child's device and take it to your room for the evening, take a few minutes to review their online activity. This is a more in depth search than the quick spot check we did in step 3. Look through their social media accounts, email, messages, installed apps, and browsing history.

Step #5: I found a problem, now what?

I receive email and Facebook messages from parents all over the United States after they have found some disturbing activity on their child's phone. Here is a message I received from Mary, a parent that went to my parent seminar at her daughter's school.

"Hi, my name is Mary and I recently discovered that my 14-year-old daughter is been sexting a freshman at her high school. This was in December. I took away the phone but she still has a Chromebook that is required by school and has access to chat rooms. I recently logged on my phone that is linked to her accounts, and I can see her messages. Within the last month I discovered that she's been sexting with an older man. In December, when I first discovered the phone, I went to the school. They said it was a gray area and they couldn't help me and referred me to the police officer on site. I'm desperate, angry, upset, and devastated. I don't know who to turn to. I hope you can guide me in the right direction."

Mary's story is not unique. She shares the same feeling of anger, sadness, and desperation every parent who has contacted me feels when they find something alarming on their child's phone. If you find yourself in a similar situation, do not panic. Kids make mistakes, but it doesn't have to define them. Every situation is different. Unfortunately, there isn't a simple decision tree we can follow to resolve every conceivable situation. Here are some suggestions to help guide you in the right direction:

- In cases of bullying or other inappropriate behavior that involves another student, try contacting the other parent first. If that is impossible or unsuccessful, consult with your school's administrator.
- For sexting, drug use, self-harm, or other high-risk behavior, contact your school's police officer and school counselor for help.
- All threats of violence must be immediately referred to your local police agency.



Popular Apps & Games

Choosing the right social media app or game for your child is essential in keeping them safe in their digital world. This chapter of the book will give you our recommendations and parental control settings for some of the most popular social media apps and games. There are always new games and apps appearing on your child's radar. If you cannot find the app your child is asking for here, then visit our website, www.cybersafetycop.com, for up-to-date app reviews and guides.

Before we can discuss which app is safe or should not be allowed on your child's device, you must have a password-protected app store that your child cannot access on their own. Before you "approve" an app, ask:

1. Is this app age appropriate?

Some content can contain drug use, violence, and pornography even when the app store says it is rated for children 12 and older. Also, the minimum age for social media like TikTok, Instagram, etc. is 13, which was established by the Children's Online Privacy Protection Rule ("COPPA").

2. If my child is posting images and other personal information, can it be made private?

As explained in the chapter, Online Reputation & Privacy, the privacy setting is the part of a social networking website, internet browser, piece of software, etc. that allows you to control who sees information about you. A "private" setting blocks casual viewing of your social media's content. A user must first ask for permission to be granted access to your content, then you can decide to allow then in or not. A "public" or "open" privacy setting gives everyone access to the account's content, without needing to ask for permission.

3. Can strangers or anonymous people contact my child through this app?

If a stranger or someone who is anonymous can interact with your child online, you will predictably expect to find bullying, threats, and predatory behavior. Parental controls are often helpful in blocking this from happening.

4. Can I review or monitor what my child is sending or receiving on this app?

Lastly, can you check up on what your child is doing online? Have you installed an app, like Bark, to monitor and alert you to troubling behavior? If the answer is no, then you will not be happy with the outcome. In this scenario, you are waiting to be told by your school principal, school police officer, or other parent that your child needs help. Picking up the pieces after weeks or months of trauma is infinitely more difficult than intervening before things spiral out of control.

If you can not sufficiently answer the above four questions, then you should seriously consider not allowing the app on your child's device.



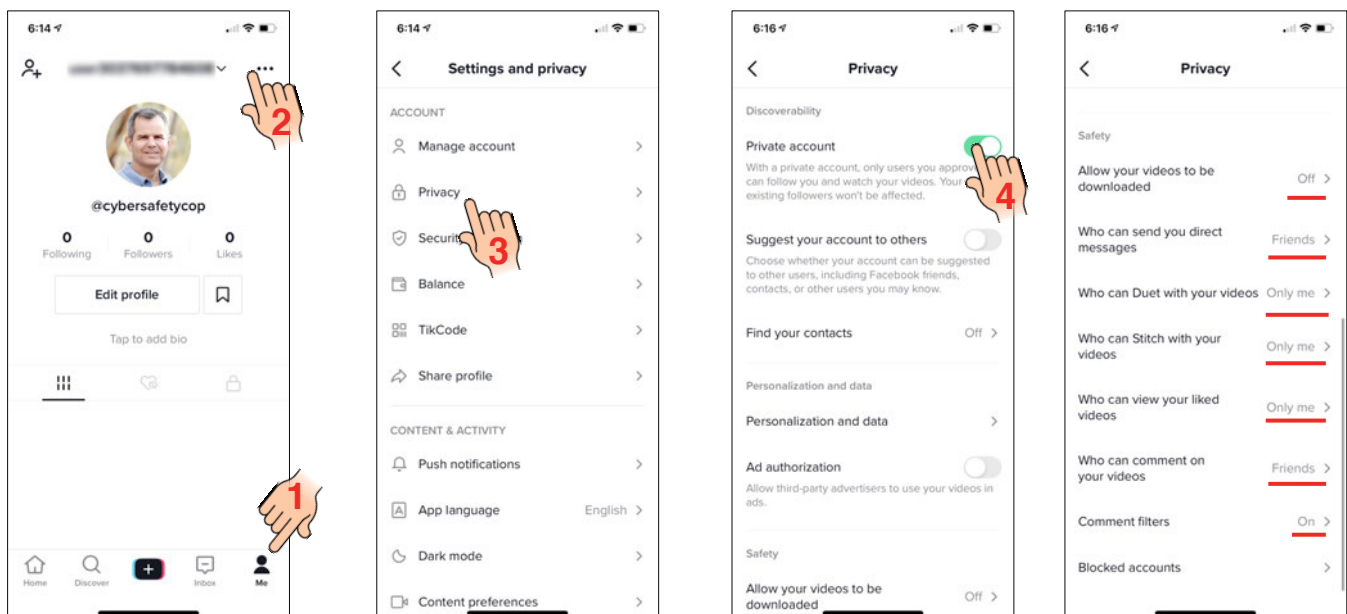
TikTok (Rated 12+, Social media, Image and Video Sharing)

App Store Description: “TikTok is a global video community. We make it easy for you to watch awesome short videos AND you can also make your own videos by capturing those funny and memorable moments to share with the world. Spice up your videos with our special effects filters, fun stickers, and so much more. Life’s moving fast, so make every second count.” Although the App Store rates TikTok for children 12+, the app’s creator recommends users be age 13+. The app isn’t classified as social media, but it must still comply with COPPA and underage data collection. Even a 13-year-old middle school student is potentially at risk using this app unless parents are well aware of the various problems.

Problems: After you download TikTok and open it on your phone, a video will start playing right away without you even selecting one. To explore further, try the magnifying glass icon next to the home icon, where you can search keywords and hashtags—yes, TikTok uses hashtags. Searching with the typical problematic hashtags often reveals inappropriate images and videos. After experimenting, we didn’t find much. There is no guarantee this will always be the case.

As for the appropriateness of the typical content, bad words and sexual lyrics that you find in popular music are often lip-synced by a child. There have also been some reports of videos depicting self-harm and violence, on the app.

Parental Controls: If your child is going to use this app, you must turn on the parental controls. TikTok also has a feature called Family Pairing. Family Pairing links a parent's TikTok account to their teen's and once enabled, they will be able to control Digital Wellbeing features.



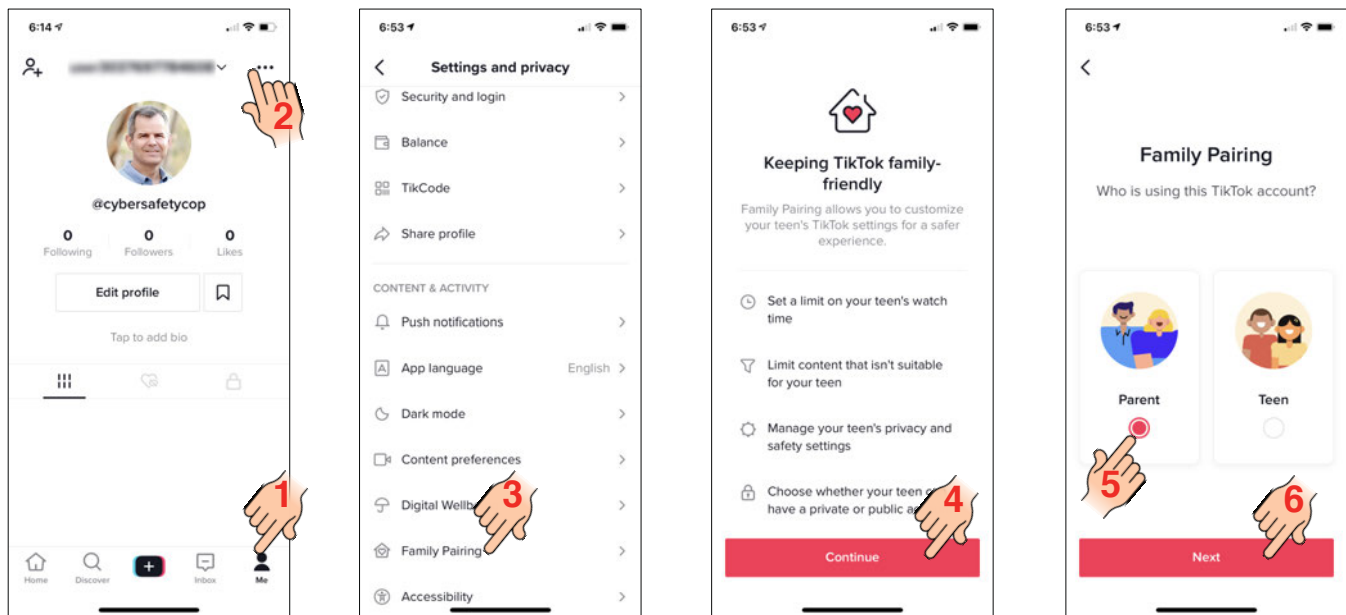
1. Set the privacy setting to private by following steps 1 through 4.
2. Make sure the safety settings are set as shown in the last step.

With a private account, your teen can approve or deny followers and restrict their uploaded content and incoming messages to followers only. If your teen has a public profile, anyone signed into TikTok can view that user's public videos. However, only approved followers can send them a message.

Please remember: Even with a private account, profile information – including profile photo, username, and bio – will be visible to all users. Counsel your teen not to reveal personal information such as age, address, or phone number in his/her profile.

In addition to the parental controls on your child's app, TikTok also has an essential parental control feature called, Family Pairing. Family Pairing links a parent's TikTok account to their teen's and once enabled, they will be able to control TikTok's Digital Wellbeing features.

To enable Family Pairing, two devices are required: a parent or guardian's logged-in TikTok account as well as the teen's logged-in TikTok account. Follow the steps below on the parent's device:



Stop when you have the QR code displayed on the parent's device. Now, it's time to link the child's TikTok app. Open the child's TikTok app and navigate to Family Pairing in the settings, just as you did on the parent's device. Choose Teen, and then click Next. Scan the QR code from the parent's device and then choose to link accounts. Now, from the parents device, you can manage TikTok screen time, restrict inappropriate content, turn off search, and manage privacy. These settings cannot be undone by the child's device.

Recommendation: *Safe for children 13+ with parental controls and parental supervision.*



Instagram (Rated 12+, Social media, Image and Video Sharing)

Instagram is a social media app used to share photos and videos through Stories, Feed, Live, IGTV or Direct messaging. The minimum age to have an Instagram account is 13.

Problems: Instagram is one of the most common social media apps found on teens' devices, which

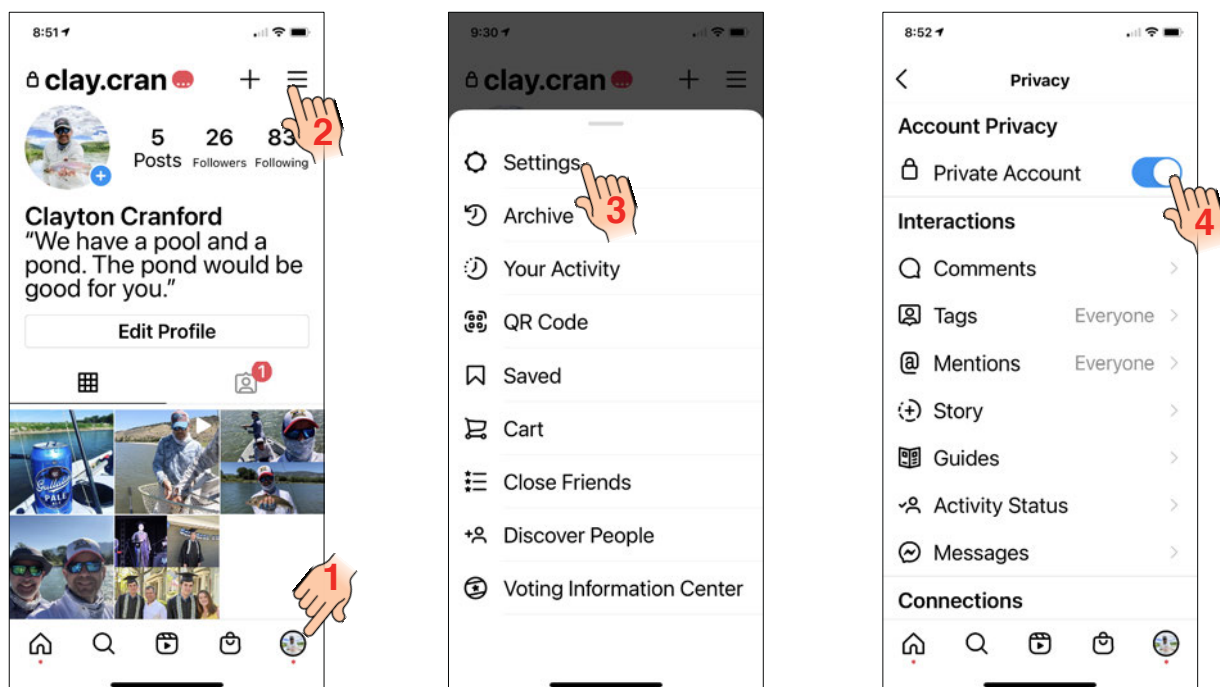
puts it on the front lines of cyberbullying, threats, and sexting. Instagram does not have parental controls in the traditional sense, which makes it more difficult for parents to manage and support their child on it than an app like TikTok.

There is a lot of inappropriate content on Instagram, including pornography. Unfortunately, you cannot filter it out.

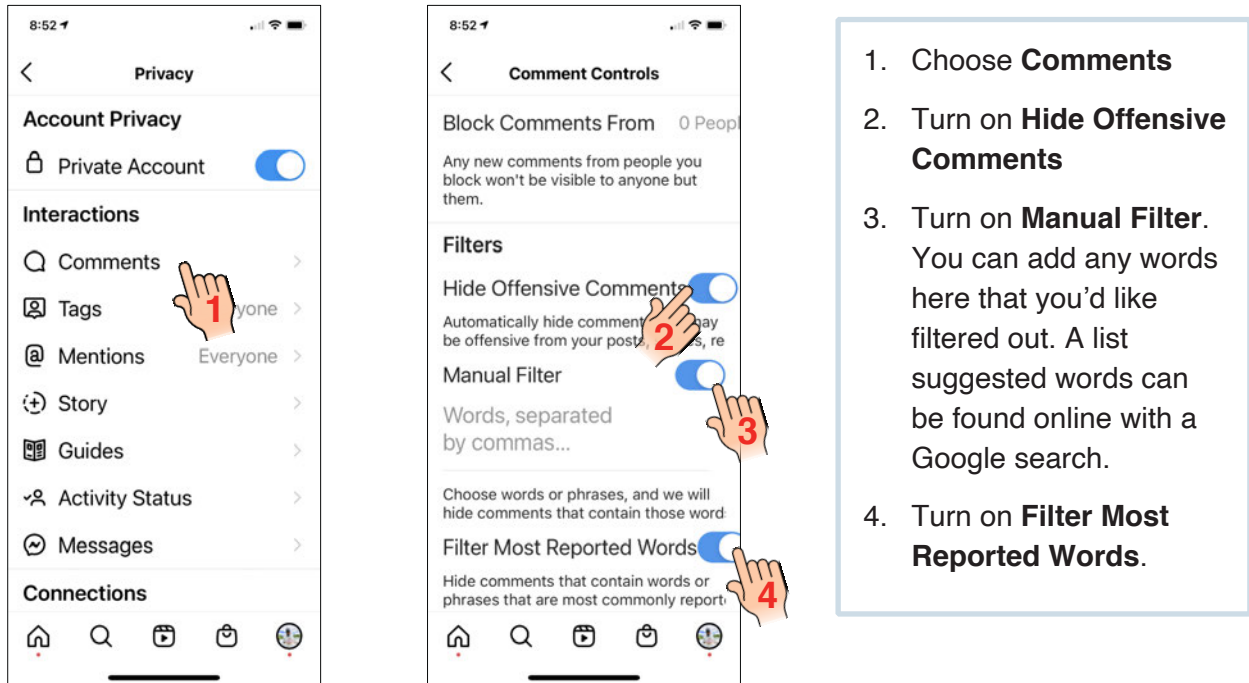
Instagram has an instant messaging feature called Direct Messages. You might have heard teens talk about “DM’s,” this is slang for Direct Messages. If you are only following your child on Instagram, you are not seeing what is happening in the DM’s. Your child knows this, so this is where a lot of the problems are. You can chat with one person or in a group. You can send text, images, or videos. Instagram has a messaging featured called Vanish Mode. It is Instagram’s take on Snapchat’s disappearing messages. Turning on Vanish Mode allows you to send messages that will self-destruct after everyone in the message thread has seen them. Similarly to Snapchat, Instagram will send a notification if the recipient takes a screenshot (nothing will notify you if someone takes a picture of a screen using a different phone’s camera) of the message sent in Vanish Mode. Also, you can report a message as abusive even if it has already disappeared. You cannot disable Vanish Mode feature. You cannot stop your child from sending or receiving disappearing messages. Even if your child has a private account, strangers can still message them.

Parental Controls: As mentioned earlier, Instagram does not have parental controls. There are settings that will make your child safer on Instagram. Unfortunately, your child can change any setting to their liking. At the time of this book’s publication, there is no way to lock those settings from being tampered with. I hope Instagram will change this in the near future.

The first setting to making Instagram safer for your teen is the Account Privacy setting. All of your child’s social media accounts, not just Instagram, should be set to Private. Follow the steps below:



Second, manage interactions in the Comments settings. Follow the steps below:



Knowing how to report abusive comments, accounts, or inappropriate content is an important skill. All reporting on Instagram is anonymous. Encourage your teen to report content or behavior that is harmful. Here is how you do it:

How to report the entire account

Tap the ... button in the top right corner of the offending user profile.


Tap **Report**. Then tap **Spam** or **It's inappropriate** (depending on the reason for the report), and then choose the follow up questions that best describes why this account should be reported. You can also **block** this account here too.

How to report individual posts

Tap the ... button in the top right corner of the offending post.

Tap **Report**. Then tap **Spam** or **It's inappropriate**. Then, choose whatever path best fits the reason for you reporting the post. You can also **block** this account here too.

How to report individual comments

Swipe left on the comment itself and tap .

Tap **Report this Comment**, and then follow whatever path best fits the reason for you reporting the comment. You can also **block** this account here too.

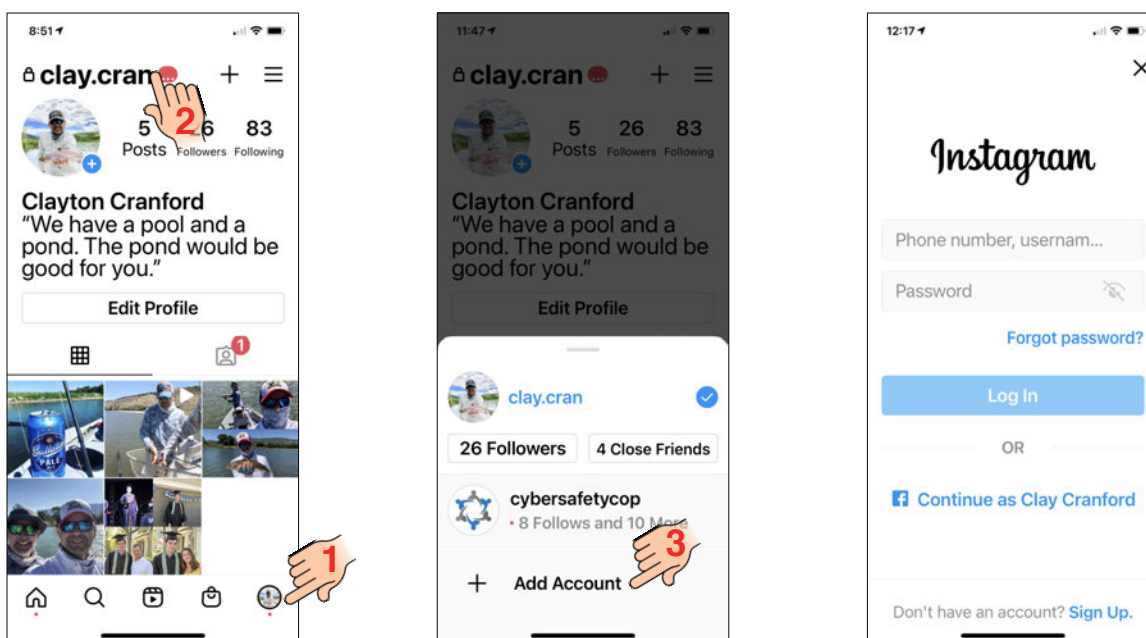
Secret Instagram Accounts “Finstas and Spam Accounts”

It is not uncommon for teens to have more than one Instagram for completely innocent reasons. They are commonly known as “finstas,” or fake Instagram accounts. It comes down to secrecy and image,

but mostly image. Teens will create multiple accounts with their followers in mind. They may have an account that everyone at their school follows. The images and stories posted in a place like this will be highly curated and edited to make the teen look as cool and fabulous as possible. Obviously, the images and stories are misleading and make the person look more amazing and fun than they are in real life. Wonder why teens get depressed when they look at their social media? They think their life is horrible based on what everyone else is posting, but of course the person they are admiring is doing the same thing when they look at their social media. Fame and beauty on Instagram is an illusion. Teens will create other accounts, often called “spam” accounts for a much smaller group of friends. They may need more than one spam account to accommodate different friend groups. For instance, a student might have a spam account for their friends on their sports team, and another for their church youth group. Teens may even create an account that they let their parent know about, and carefully only share content that is “parent safe.”

How will I know if my child has a secret Instagram account?

First, I recommend logging into your child’s Instagram account on your device. The Instagram app will allow you to have up to five accounts logged into your app simultaneously. Instagram doesn’t care if two or more people are logged into the same account at the same time. Follow the steps below to add additional accounts to your Instagram app:



1. Go to your Profile page by tapping on your **profile icon** button in the bottom left corner of the app.
2. Tap on your **username** at the top of the app.
3. A panel opens at the bottom of the app. Tap **Add Account** to add another account to your app. You must have the username and password to do this.

Discovering secret accounts

Follow the same steps on your child’s device. All of their accounts will be listed just above the Add Account button.

Are there parental apps that will help me manage Instagram?



Yes, there are parental control/notification apps available to help you protect your child on Instagram. **Bark** is the best one on the market and I've been using it on my children's phones for a couple of years now. It works on both iPhones and Android powered phones. It will run in the background, passively monitor direct messages and comments, and then alert you when it detects dangerous activity.

I have a promo-code for you. Enter "cybersafetycop" when you sign up to get 15% off your subscription forever. Bark is available on the Apple App Store, Google Play, and at www.bark.us.

How and when should I give Instagram to my teen?

My first recommendation is to wait as long as you can to give them Instagram. I'd recommend your child be in high school before they get Instagram. Whenever you decide to give them Instagram, tell them there are a few rules they must follow if they want an account:

1. You (as the parent) get to know the username and password to ALL of their accounts, even the finstas.
2. The account must be Private.
3. Their followers must be people they know in real life (IRL), and people they trust.
4. They are not allowed to use Vanish Mode or any other disappearing messages.
5. You (as the parent) have 100% access to their phone and Instagram account anytime you desire to look.

Lastly, tell them if they don't live up to these rules, there will be consequences. Tell them up front what the consequences will be. Whatever it is, make sure it is a sufficient deterrent to disobeying the rules, and something you can reasonably follow through on. You must follow through on the discipline.

Recommendation: *Safe for children 14+ with parental controls and parental supervision.*



YouTube (Rated 17+, Video streaming and sharing, social media)

App store description: "YouTube is a video sharing service where users can watch, like, share, comment and upload their own videos. The video service can be accessed on PCs, laptops, tablets and via mobile phones."

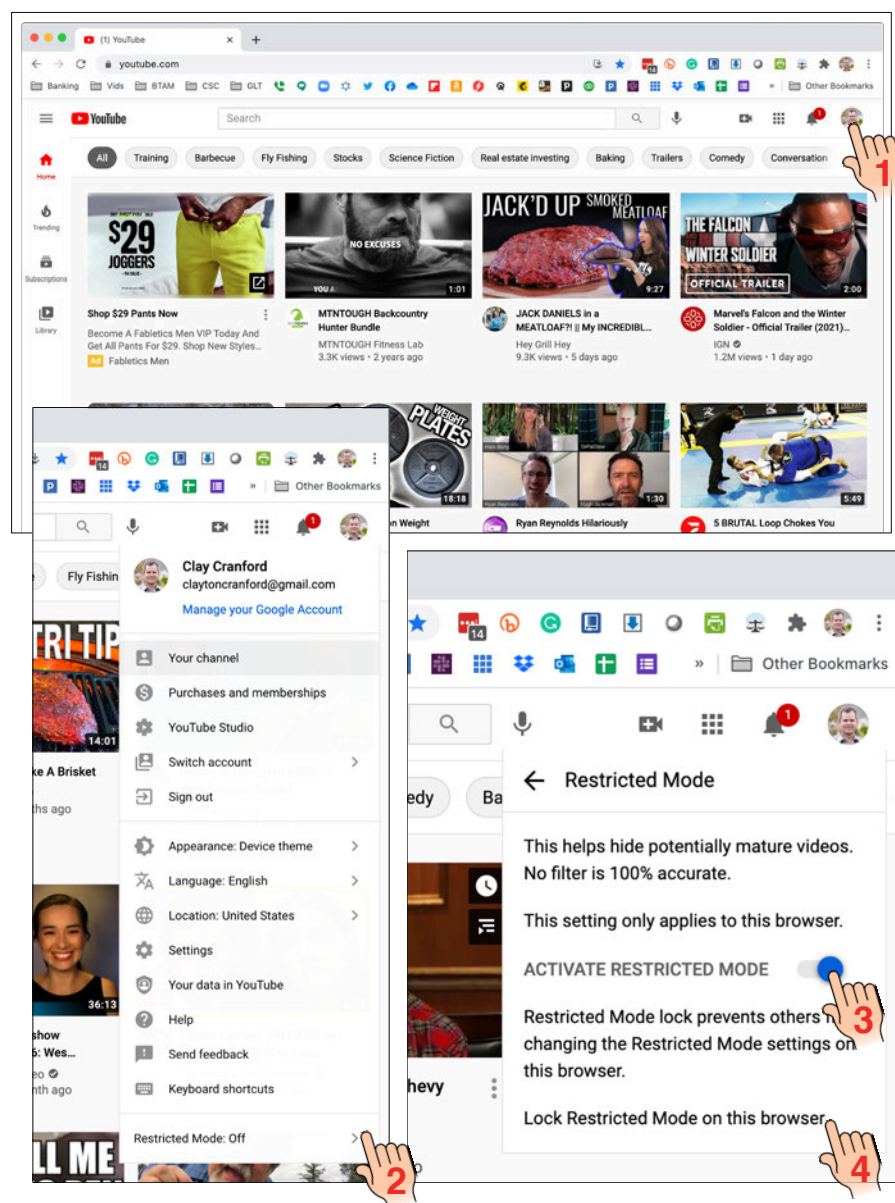
Problems: YouTube is always in the top three most used apps by children. It is fair to say that parents have a love/hate relationship with this app. Excessive screen time is an issue with this app. Children burn a lot of time watching the never ending stream of videos. Every video ends with a suggestion for another video, and another video. What makes screen time regulation difficult is the fact that many schools and teachers are using it as a source for educational videos.

Many parents have learned the hard way that a lot of the content on YouTube is not for young children. I often have parents reaching out to me for advice after their elementary-aged child is exposed to graphic content. An often asked question from parents is what is the appropriate age for an

unsupervised child on YouTube? Unless you are sitting next to your child while they are watching Youtube, you cannot effectively control what they can see. Youtube's app description rates their app as appropriate for ages 17+. What is the appropriate age for an unsupervised child on YouTube? The same age you would let your child watch an R-rated movie. Everything they can see in an R-rated movie they can see on YouTube.

Parental controls: YouTube does have a kind of filter called restricted mode. My experience is that it is not 100%, but should still be enabled. Follow the steps below:

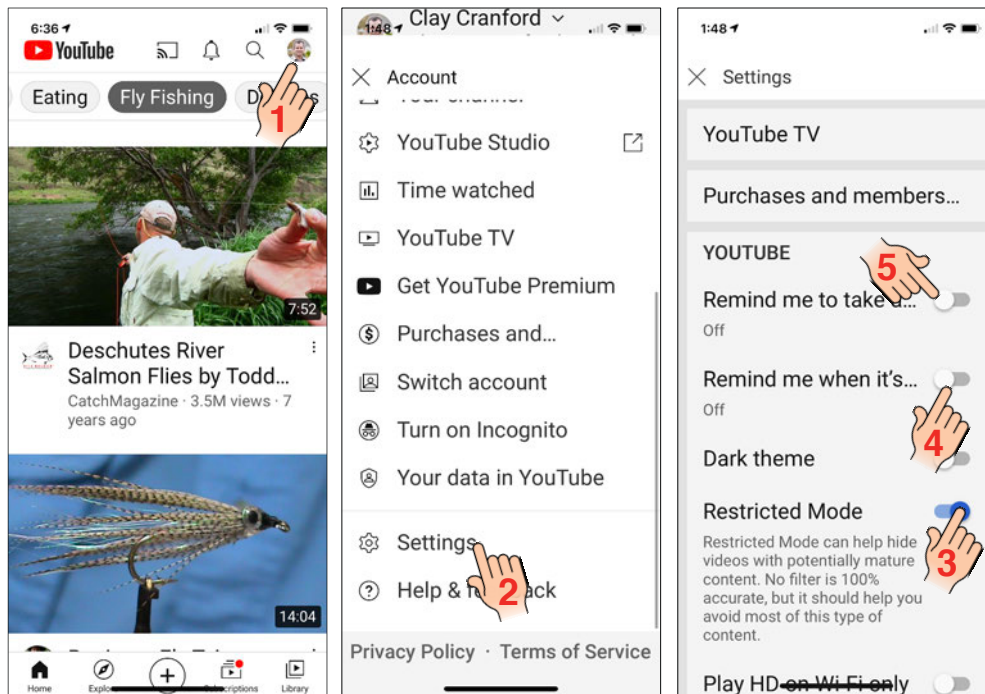
Desktop Version



You must be logged into the YouTube account your child will be using.

1. Click your **profile image**.
2. Click on **Restricted Mode** arrow.
3. Click the **Activate Restricted Mode** slider to on.
4. Click **Lock Restricted Mode on this browser**.
5. Enter your Google account's password to lock Restricted Mode on.

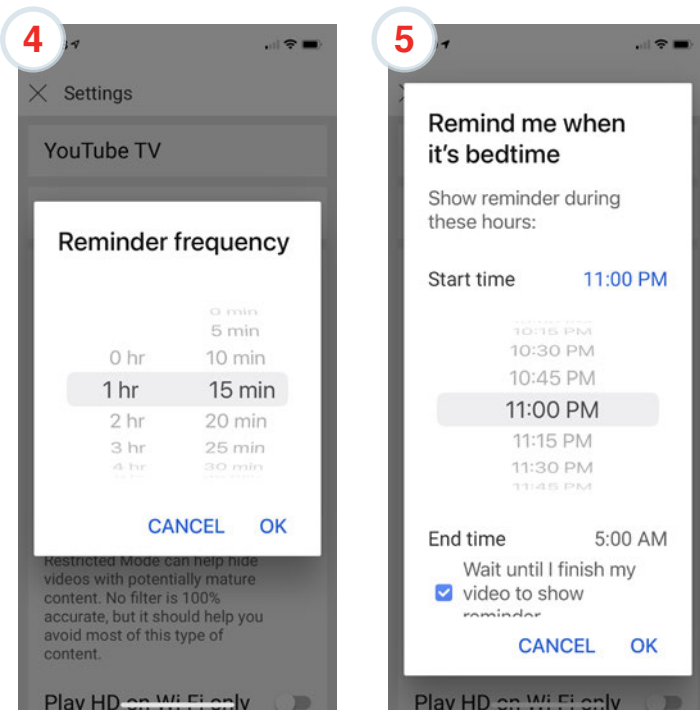
Mobile App Version



You must be logged into the YouTube account your child will be using.

1. Click your **profile image**.
2. Click on **Settings**.
3. Click the **Restricted Mode** slider to on.

Note: You cannot lock restricted mode on the mobile app.



You can also set helpful reminders for screen breaks and for bedtime. These are only reminders, they will not turn off YouTube.

4. Turn on **Remind me to take a break** to set a reminder alert when you've been watching too long.
5. Turn on the **Remind me when it's bedtime** to set an alarm to go to bed.

Recommendation: Use with caution. Safe for children 13 to 15 with parental controls and parental supervision; Safe for children 16+ with parental controls and occasional parental supervision. For children under 13, use Youtube Kids App.



YouTube Kids (Rated 4+, Video streaming)

App store description: YouTube Kids was created to give kids a more contained environment filled with family-friendly videos on all different topics, igniting your kids' inner creativity and playfulness. Parents and caregivers can guide the journey as your

kids discover new and exciting interests along the way.

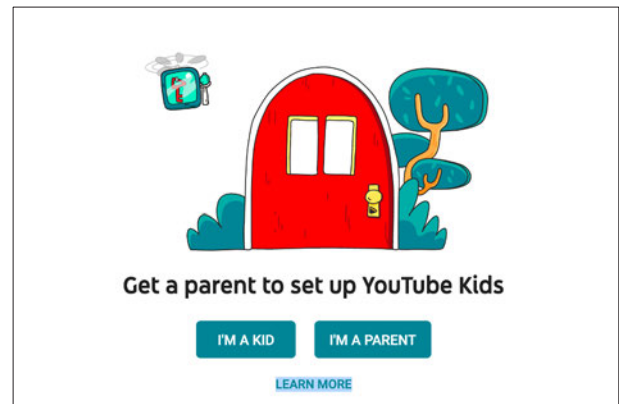
Problems: No significant problems. YouTube has improved their video selections and parental controls.

Parental Controls: YouTube Kids allows signed in parents to create a separate profile for each kid in their household. Each profile has a separate set of viewing preferences and recommendations, allowing multiple kids to get the most out of the YouTube Kids app.

Profiles are available on any device where the parent is signed in and the YouTube Kids app is installed. [Learn more.](#)

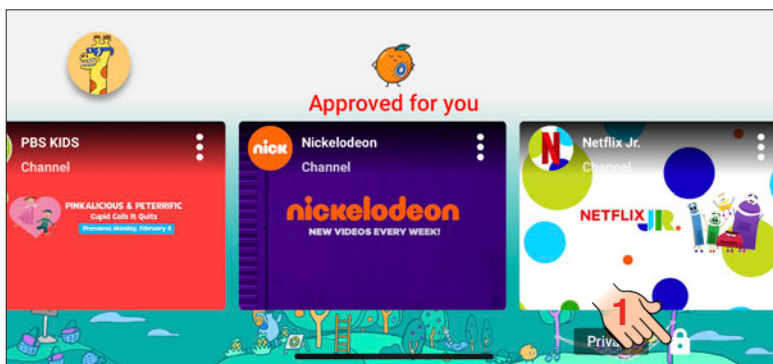
To create a YouTube Kids profile for your child, you go to www.youtubekids.com or use the YouTube Kids app available on Apple's App store or Google Play. The following instructions are for the website, but the app setup is identical.¹



1. Open the YouTube Kids app or go to www.youtubekids.com, and follow the on-screen instructions.
2. When you're asked to, enter the year you were born.
3. Choose whether or not to sign into the app to get greater access to features and parental controls. I highly recommend you sign into your Google account. If you do not yet have a Google Account, add or create a Google Account by following the prompts. After you add your account, tap **Sign In**.
4. Set up a profile for your child. When you provide a month of birth, the app will use this to more accurately provide an age-appropriate experience. Only you and your child can see this info.
5. Select a content experience for your child.
 - Preschool (Ages 4 & under)
 - Younger (Ages 5-7)
 - Older (Ages 8-12)
 - Approve content yourself
 - The Preschool content setting (ages 4 & under) allows kids to watch videos that promote creativity, playfulness, learning, and exploration. Search results in Preschool are limited to content recommended for kids 4 and under. Our systems work hard to exclude content not suitable for kids in preschool, but not all videos have been manually reviewed. If you find something inappropriate that we missed, you can block it or flag it for fast review.



- The Younger content setting (ages 5-7) allows kids to search and explore songs, cartoons, crafts, and more. Our systems work hard to exclude content not suitable for young kids, but we can't manually review all videos. You may find something inappropriate that we missed. With this setting, search results will be limited to content for kids 7 and under. Please note, if you wish to turn Search off, you can do this following the instructions in parental settings.
- The Older content setting (ages 8-12) allows kids to search and explore additional music videos, gaming, science, and more. Our systems try to exclude mature content, but we can't manually review all videos. You may find something inappropriate that we missed. With this setting, search results are limited to content recommended for kids 12 and under. Please note, if you wish to turn off the Search feature, you can do this following sign up in parental settings.
- With Approve content yourself, your child will only be able to watch videos, channels, or collections that you've approved. Collections are videos and channels grouped by topics such as science and music. With this setting, your child won't be able to search.

Note about choosing the right content profile for your child: If you choose between the three age-based content settings (i.e., Preschool, Younger, and Older), you are relying on YouTube to manage what they see. This is how they describe it, "Our automated systems select content from the broader universe of videos on YouTube. We work hard to exclude content that's not suitable for kids, but we can't manually review all videos and no automated system is perfect. If you find something inappropriate, you can block it or report it for fast review." YouTube Kids has not had a perfect record of keeping inappropriate videos from getting into their video feed. For the safest and most restrictive setting, we recommend choosing **Approve content yourself** and turn **search** off. You can always change the content settings. We also recommend using a **custom passcode** and not the easily defeated multiplication challenge.




1. Tap the  in the bottom corner of any page in the app.
2. Complete the multiplication problem or read and enter the numbers that appear. Or, enter your custom passcode.
3. Select  Settings .

Changing parental control settings after setting up your child's profile Approved Content Only

In this setting, your child will only be able to watch videos, channels, and collections that you've handpicked. Collections are videos and channels grouped by topics, such as science and music, picked by the YouTube Kids teams or by our partners.

1. Select your child's profile and enter your parent account password to modify settings.

2. Select **Approved content** only to enable.
3. Review the info in the “Getting Started” pop-up.
4. Select **Select**.
5. Tap the  icon on any collection, channel, or video to approve content you’d like to make available to your child.
6. Select **DONE** in the red box at the bottom of the screen to exit.

Note: You can edit the list of collections, channels, and videos you’ve approved at any time by tapping **Manage** under the “Approved content only” setting. While you're approving content, you can preview what your child's experience will be like by tapping **PREVIEW**. You can also turn off “Approved content only” at any time by returning to Settings.

Turning search off

You can restrict your child’s experience to a more limited set of videos by turning the Search feature off.

With the Search feature turned **off**, your child can’t search for videos. Your child will also be limited to videos and channels that have been verified by YouTube Kids.

With the Search feature turned on, your child can search for new videos that interest them from the millions available in the YouTube Kids app.

Note: Please keep in mind that there's always a chance your child may find something you don't want them to watch. You can report this content for quick review.

To turn off the Search feature, toggle Allow searching to **Off** in Settings .

If you turn the Search off, the watch and search history in your app will be cleared. This will reset Recommended videos and Watch it again.



Snapchat (Rated 13+, Social media, Image and Video Sharing)

This extremely popular app which allows the user to send a picture, text, or video to another Snapchat user. What makes this app special is that the sender can assign a lifespan to the message, up to 10 seconds.

Problems: First, Snapchat can send self-destructing messages that disappear after the recipient opens the message and the timer counts down to zero. This gives the sender the impression that they can send a “snap” without the consequences of sending an inappropriate image or video. Snapchat is the number one sexting app. Images can be captured in a screen shot or by taking a picture with a second device. Second, by default, Snapchat shares the user’s exact GPS location on a map, which is found on the search screen of the app. This feature shares the user’s GPS location 24/7 even if they are not actively using the app. It runs in the background. This can be blocked by turning on Ghost Mode. Ghost Mode cannot be locked by parents. This feature can be turned on or off at any time by the user. Third, Snapchat has a password protected folder called, “For MY Eyes Only.” Any image or video

can be moved here and can only be seen with a four-digit pin code created by the user.

Parental Controls: None.

Recommendation: *Not safe for children of any age.* I would highly recommend parents not give this social media app to their children under the age of 18-years-old.



Discord (Rated 12+, Social Media, Gaming, Video and Audio Streaming, Chat)

Discord describes itself as: “a free voice, video, and text chat app that's used by tens of millions of people ages 13+ to talk and hang out with their communities and friends. The vast majority of servers are private, invite-only spaces for groups of friends and communities to stay in touch and spend time together. There are also larger, more open communities, generally centered around specific topics such as popular games like Minecraft and Fortnite. All conversations are opt-in, so people have total control over who they interact with and what their experience on Discord is.”

You must be 13-years-old to have a Discord account. Discord’s website: “Discord is a communications service for teens and adults who are looking to talk with their communities and friends online. We do not allow those under the age of 13 on our service, and we encourage our users to report accounts that may belong to underage individuals.”

Discord has its own vocabulary. You might hear your teen or students using these words when talking about Discord.

Server: Servers are the spaces on Discord. They are made by specific communities and friend groups. The vast majority of servers are small and invitation-only. Some larger servers are public. Any user can start a new server for free and invite their friends to it.

Channel: Discord servers are organized into text and voice channels, which are usually dedicated to specific topics and can have different rules.

- In text channels, users can post messages, upload files, and share images for others to see at any time.
- In voice channels, users can connect through a voice or video call in real time, and can share their screen with their friends - we call this Go Live.

DMs and GDMs: Users can send private messages to other users as a direct message (DM), as well as start a voice or video call. Most DMs are one-on-one conversations, but users have the option to invite up to nine others to the conversation to create a private group DM, with a maximum size of ten people. Group DMs are not public and require an invite from someone in the group to join.

Go Live: users can share their screen with other people who are in a server or a DM with them.


Problems: If your kid is a gamer, they will want this app. It is intended for teens to chat about their games and create a talk-group when they are playing a coop game. Teens can access Discord via their PC, browser, or mobile phone. Once there, they can join a chat they've been invited to or they can

create private servers and invite their friends to play and discuss games by voice, text or video. They can also message each other individually or in group chats.

There is the potential for a lot of stranger interaction on Discord. Predators know one of the best ways to build a relationship with a child and groom them to be sexually exploited is through online gaming. Discord is, and continues to be, fertile ground for predators. I have counseled dozens of parents over the past couple of years who have had their child exploited by a predator on Discord. In 2020, 10 men were arrested and sentenced for utilizing private servers to produce and exchange child pornography on Discord. They actively worked together to identify minor females' social media platforms and profiles, including girls as young as 10-years-old and strategized how to convince the children to engage in sexually explicit activity via live web camera. While pretending to be minor boys and girls, the predators streamed pre-recorded videos of other underage minors engaging in similar conduct to the targeted victims in an effort to get the children to believe they were watching a live video of someone their own age. The victims were unaware that they were communicating with adult men who were recording their sexually explicit activity. After successfully recording a victim, the defendants shared the sexually explicit videos with each other by uploading the files to file-storage sites and placing a link to download the file on a section of their private Discord server. There were more than 172 victims.¹

Pornography can be easily found on Discord's private servers. I have counseled many parents who have blocked porn sites on their children's devices to learn their child had been consuming an unlimited amount of pornography in a Discord private server.

Parental Controls: There are privacy settings that will help limit who your child can chat with and possibly filter out explicit content from DMs.

To access the privacy settings, click on the  icon next to the account name, which is at the bottom left of the screen (desktop browser version), then click on **Privacy & Safety**.

Safe Direct Messaging

Here you can block direct messages that contain explicit media content.

- **Keep me safe** - With this setting, images and videos in all direct messages are scanned by Discord and explicit content is blocked. This setting is on by default.
- **My friends are nice** - With this setting, all direct messages sent by users who are not on your Friends List are scanned and explicit content is blocked. This setting is good for those who trust their friends not to send content that they wouldn't want to see.
- **Do not scan** - With this setting, none of the direct messages you receive will be scanned or blocked for explicit content.

Block unwanted messages

- You might only want certain people to contact you. By default, whenever you're in a server with someone else, they can send you a direct message (DM).

- You can toggle **Allow direct messages from server members** to block DMs from users in a server who aren't on your friends list. If you have joined any servers prior to turning this off you'll need to adjust your DM settings individually for each server that you have joined.
- To change this setting for a specific server, select **Privacy Settings** on the server's dropdown list and toggle **Allow direct messages from server members**.

Friend request settings

This setting allows you to determine who can send you a friend request.

- **Everyone** - Selecting this means that anyone who knows your Discord Tag or is in a mutual server with you can send you a friend request. This is handy if you don't share servers with someone and you want to let them friend you with just your Discord Tag.
- **Friends of Friends** - Selecting this means that for anyone to send you a friend request, they must have at least one mutual friend with you. You can view this in their user profile by clicking the Mutual Friends tab next to the Mutual Servers tab.
- **Server Members** - Selecting this means users who share a server with you can send you a friend request. Unselecting this means that you can only be added by someone with a mutual friend.

If you don't want to be open to ANY requests, you can deselect all three options. However, you can still send out requests to other people.

Blocking other users

When you block someone on Discord, they will be removed from your friends list (if they were on it) and will no longer be able to send you DMs.

Any message history you have with the user will remain, but any new messages the user posts in a shared server will be hidden from you, though you can see them if you wish.

On desktop:

- Right-click the user's @Username to bring up a menu.
- Select **Block** in the menu.

On mobile:

- Tap the user's @Username to bring up the user's profile.
- Tap the three dots in the upper right corner to bring up a menu.
- Select **Block** in the menu.

Important note on Discord's parental controls

- There is no way to lock these settings. Your child could change them at any time.

- There is no way to restrict your child from joining a private server that contains explicit media.

Recommendation: *Minimum safe age is 16-years-old.* If you are concerned about your child's potential access to pornography or other explicit material, or you don't have the time to actively monitor your child's Discord activity, then this social media app is not for you.

If you allow your older teen to have Discord, I suggest you check up on their activity by logging into their Discord account with their username and password. By logging in as your child, you can see the servers they have subscribed to in the far left-hand column. You can also review who their friends are and any direct messages from the app's home page.



Kik Messenger (Rated 17+, Social Networking, Instant Messaging)

Kik Messenger is a free instant messaging and social networking app that uses your smartphone's data plan or Wi-Fi connection to send messages to other Kik users, bypassing SMS (short message service). It's available on iOS, Android, and Amazon for Kindle Fire. Kik emphasizes privacy and anonymity. As of 2016, Kik Messenger had some 300 million registered users, and was used by an estimated 40% of teenagers in the U.S. It hasn't disclosed any user figures since 2016.

Problem: Kik has a long history of predators using it to exploit children. In 2019, it looked like Kik was going out of business, but in the eleventh hour, it was purchased by a US company. Some of the features that made the app dangerous were taken out; however, chatting via text or video with strangers is still possible. There are websites dedicated to matching strangers on Kik to share nude images.

Parental Controls: None

Recommendation: *Not safe for children of any age.*

Note: Any instant messaging app that can be downloaded from the app store (e.g., Signal, Telegram, WhatsApp, etc.) will probably not be appropriate for a child. Most messaging apps facilitate stranger interaction coupled with anonymity. If your child want to text a friend, I recommend only using the messaging app that comes with your phones operating system. Bark can effectively monitor the text messaging app that came with your phone.



Reddit (Rated 17+, Chat, Discussion Board)

Reddit is rapidly becoming a social media platform teens and young adults are using to discuss topics that are important to them with likeminded individuals. For young people, it is a primary source for news, information, and entertainment, and most parents have never heard of it. The concept is simple: Reddit users post whatever they want (including images and videos) in message boards, called subreddits, and other users comment and up or down vote the post. The most popular stories or posts become more visible and generate more discussion. If a post generates enough discussion, it can be viewed on Reddit's homepage, known as the main-reddit. A subreddit is preceded by the characters "r/" in the URL. For example, "r/planes" would be a subreddit

on the general topic of planes.

Similarly, a subreddit entitled “r/stocks” would be all about the stock market. Do you want to discuss or find information on literally any topic? You will likely find a subreddit for you, or if you don’t, you can start your own subreddit.

Reddit is a website and a mobile app available for all mobile devices. Anyone can browse Reddit and its subreddits, but to post, comment, up/down vote, or start a new subreddit, you must be a registered user.

Problems: Can my child talk to strangers on Reddit? Yes. Reddit’s mobile app has a direct chat feature and chat rooms. There is no way to know who your teens are talking to on Reddit. Redditors rarely post under their given name, and there is no verification of identity (unless you’re hosting an AMA – Ask Me Anything). That means it can be a dangerous place for young people, and a nightmare for parents, mainly since Redditors often do in-person meet-ups.

Porn and other forms of inappropriate content can readily found on Reddit. Anything goes on Reddit, provided it is not illegal material like child pornography. Many subreddits are tagged with NSFW. This acronym stands for “Not Safe For Work.” Reddit’s content policy guidelines for NSFW to include: “Content that contains nudity, pornography, or profanity, which a reasonable viewer may not want to be seen accessing in a public or formal setting such as in a workplace should be tagged as NSFW. This tag can be applied to individual pieces of content or to entire communities.”

Parental Controls: Reddit does not have traditional parental controls. NSFW search results and the ability to view NSFW subreddits can be turned off in the account settings. The only problem is that the blocked user can easily get around this parental control. If your teen wants to see NSFW content, all they have to do is go into settings and uncheck that parental control, or create a new account the parent doesn’t know about.

Recommendation: *Not safe for children of any age.*



Houseparty (Rated 12+, Group Video Chat)

App store description: Houseparty is the face-to-face social network where you can connect with the people you care about most. The app makes connecting face to face effortless, alerting you when your friends are “in the house” and ready to chat so you can jump right into the conversation. The same goes for you opening the app! Your friends will know you’re in the app and ready to chat, so they can join you (...because rejected calls are so last year). Houseparty is truly the next best thing to hanging out in person. See your friends more often on Houseparty.

Problems: People, maybe people your child does not know, can join your child’s group video chat without permission if the chat group is not locked. When a user is in a Houseparty group chat, a connection from one of the in-chat members can choose to join the group, even though they are not connected or known to the other users. Houseparty does give you the option to lock your conversations. When a conversation is locked, everyone is notified that the user has locked the

conversation, and if someone should try to join, they are blocked from doing that. If you allow your child to use Houseparty, we encourage you to get them into the habit of locking the conversation. If someone within the conversation unlocks the chat, everyone is notified that the conversation has been unlocked.

One major issue with live streaming apps is unless the parent is sitting on their kid's shoulder, they will not know what is happening or being said on the video chat, making accountability for children using this app very difficult.

Parental Controls: None.

Recommendation: *Safe for children 13 years or older.*

Topics to discuss with your child before any live video chat apps:

1. Video chats should be done in a common area of the house where the parent can freely watch and listen to what is going on.
2. All conversations on Houseparty must be locked. Your child should have a standing rule that if the conversation is ever unlocked, they must leave the chat. They are never allowed to chat with someone they don't know.
3. Talk to your child about the lack of privacy on social media, and specifically on this app. A Houseparty user has no control of what another user does, including taking screenshots of the group chat and/or video recording the conversation. Saying something inappropriate, even in jest, can have horrible consequences.
4. If one of the participants in the chat did something inappropriate, your child must leave the chat. Explain to them, although they are not the one doing the inappropriate thing, by remaining in the chat they are silently condoning the behavior.
5. Make sure that the other children's parents know that their child is having a video chat with your child.



Omegle (Rated 18+, Live Video Chat)

Omegle is an online chat website (www.omegle.com) that allows users to video chat with strangers. Their tag line is, "Talk to strangers!"

Problems: Omegle users are essentially anonymous. When you are randomly put on a live video chat with a stranger, anything is possible. Omegle's own safety disclaimer on their website states: "The people you encounter on Omegle may not behave appropriately, and that they are solely responsible for their own behavior. Use Omegle at your own peril. Disconnect if anyone makes you feel uncomfortable." It is not uncommon to find people completely nude in front of their camera. Predator behavior is commonly found on Omegle.

Parental Controls: None. You must use web filtering to block access to this website.

Recommendation: Not safe for children of any age.



Pinterest (Rated 12+, Social Networking)

Pinterest is a visual discovery engine for finding ideas like recipes, home and style inspiration, and more. With billions of Pins on Pinterest, you'll always find ideas to spark inspiration. When you discover Pins you love, save them to boards to keep your ideas organized and easy to find. When you share something on Pinterest, each bookmark is called a pin. When you share someone else's pin on Pinterest, it's called a repin. You group pins together by topic onto various boards or pinboards in your profile. Each board mimics a real-life pinboard.⁸

Pinterest has always been considered a social media site for grownups. Still, recently more and more teens are opening accounts on Pinterest to get inspiration for their crafting hobby or share their artwork.

Problems: Like all image-sharing social media platforms, you can find pornography. I recently had a parent contact me because his teenage son, who had been battling porn addiction, was going on Pinterest to find explicit images.

You can send private messages on Pinterest. Pinterest messages can only be sent to someone who is following you. And, likewise, someone can only send you a message if you are following them.

Parental Controls: None.

Recommendations: *Safe for children aged 13-years and older with parental supervision.*

If you allow your teen to have Pinterest, I suggest you check up on their activity by logging into their Pinterest account with their username and password. By logging in as your child, you can see the pins they have saved what they are sharing as well as their conversations.



Fake Calculator App (Vault Apps) (No age rating, Utilities, Privacy App)

The Calculator# App is just one of many similar apps that appear to be a legitimate calculator (or some other utility app) but is a "vault" to hide images and videos. The app store description is as follows: Calculator# is the ultimate privacy app for photos, videos, notes, and other information on your iPhone. Its deceptive and disguised design makes it impossible for hackers and other users to discover your hidden data. The app has a generic calculator icon, which prevents snoopers from identifying Calculator# on your iPhone. The next security layer involves entering a specific code inside a calculator app to access the user interface. In all, Calculator# is the most secretive and secure data privacy app you can get for the iPhone.

Problems: The problem with such an app is obvious. Vault apps are used exclusively by teens to store nude sext images, and pornography downloaded from the Internet.

Parental Controls: None. A password-protected app store will stop your child from downloading a vault app.

Recommendation: *Not safe for a child of any age.*



Yubo: Livestream with friends (Rated 17+, Live Video Streaming, Social Networking)

Yubo (Formerly Yellow) is a social media app for iOS and Android devices that lets users create a profile, share their location, and flip through images of other users in their area. You can either scroll through the current live streams or browse individual profiles by swiping Tinder-style, right on profiles you like and left on profiles you don't.

Problems: A Yubo user can browse other users' profiles, swiping left to pass or right to "like" them. Users who like each other's profiles can chat. This app is being called "Tinder for teens."

The app's terms state users must be over 13-years-old, but it's easy to fudge the date. A child on this app could be chatting with an adult pretending to be a teenager. Even the app realizes this is a potentially dangerous situation. Upon registration, the app presents users with a teen safety guide; it also sends the information to users via text message and reminds users frequently about posting appropriate content.

The app encourages users to enable their phones' location services. However, you can opt to hide your city, limiting peoples' ability to find you. The app has a built-in barrier to limit profile views by users' reported age, but that doesn't work. (It's possible, for instance, to create an account as a fifteen-year-old user and filter profile views to users ages 23 to 25) Further, the Live video chat feature lets anyone from age 13 to 25 join.

The app does not proactively shut down accounts that violate their user agreement. The app developers are waiting for a user to flag an account as "a problem" and then remove it. A casual search on Yubo using the typical inappropriate phrases will find substance use, profanity, racial slurs, and scantily clad people.

Lastly, Yubo links to Snapchat. Yubo funnels stranger interaction and relationships to Snapchat, a popular app to used for sexting.

Parental Controls: None

Recommendation: *Not safe for children of any age.*



Yolo: Anonymous Q&A (Rated 17+, Social Networking)

Yolo, which stands for "you only live once," allows teens to ask for "honest feedback" in the form of anonymous replies to a question. The app can't work without Snapchat. Users have to link their Snapchat account to the YOLO app to use it. Once they are connected, users open the YOLO app and press 'Get anonymous messages.' In Snapchat, users can send a request "send me honest messages" to their friends or their story. Friends can send you anonymous messages and questions to which you can view on the YOLO app. Replies to Yolo's anonymous messages can then be posted to Snapchat.

Problems: The problem with Yolo is very predictable. Whenever you have any form of anonymous messaging, you will have bullying, threats, and sexually explicit behavior. When a teenager knows that

no one can connect their rude Yolo answer back to them, they feel free from any responsibility or facing consequences of their behavior. Teens in anonymous environments are more likely to say or do something hurtful to themselves or others.

Parental Controls: None

Recommendation: *Not safe for children of any age.*



Twitch: Live Game Streaming (Rated 13+, Live Video Streaming)

Twitch is a viral live streaming platform primarily for gamers. Twitch's channels aren't just for gamers. You can find people live streaming how-to videos, a talk show, podcast, or performing music. If your child loves playing games like Fortnite, Minecraft, or League of Legends, they will want to watch Twitch's live gameplay.

Problems: Twitch is live, and like all live-streaming platforms, there is an element of risk to children being exposed to inappropriate content. I have spoken with many parents who were watching Twitch over their child's shoulder of someone playing Minecraft. They were shocked when the player started dropping f-bombs. It was surprising because Minecraft is a game that skews to younger children. Although Twitch has moderators and strict rules around explicit content, it doesn't offer age filters for specific categories and games, including mature, violent titles like Grand Theft Auto.

Your child can chat with strangers on Twitch. Twitch has a chat feature that runs alongside all streams. Sometimes chats are restricted to only followers or subscribers of the specific streamer. Even if you cannot actively chat, you can see what others are posting. You can hide the chat stream, but you cannot turn it permanently off. Users can also send direct messages, known as Whispers, to other viewers.

Parental Controls: Twitch does not have parental controls that can be locked. Any setting can be changed in account settings at any time.

Disable messages (Whispers) from strangers

1. Click your child's **user name** in the top-right corner of the screen.
2. From the menu that drops down, click **Settings**.
3. At the top of the page, click **Security and Privacy**.
4. Scroll down to the **Privacy** section.
5. Toggle **Block Whispers from Strangers** to **On**.

Recommendation: *Safe for high school aged children.*



Steam (Rated 12+, Game Download and Purchase, Social Networking)

Steam is a video game digital distribution service by its parent company, Valve. Steam is available on both desktop and mobile devices.

Problems: Some of the games available on Steam are not safe for children. Steam has a social network component where you can add “friends” and chat with them individually or in groups. Not all of these chat groups and community forums are game-related. Topics can vary wildly in Steam Groups, including explicit material.

Parental Controls: Steam does offer fairly robust parental controls called Family View.³ Family View is a feature for parents and families to establish their own rules for what components of Steam are accessible.

You can use Family View to limit an account's access to a subset of its content and features. With Family View, access to the Steam Store, Library, Community, Friends content and other features may be gated by the entry of an secret PIN.

Setting up Family View

1. Log into the **Steam account** your child will use.
2. Click the **Steam menu** in the top menu bar (**Preferences** on the Mac).
3. Open the **Settings** option.
4. Go to the **Family** tab on the left side of the window that opens.
5. Click **Manage Family View** to start the Family View wizard.
6. Step through the wizard to select the content and features you'd like to be accessible while in PIN-protected Family View.
7. Select and confirm your new PIN.

Family Games Library

If you've opted to only allow access to a subset of the account's library, your account's library will include a new group called Family Games. Family Games are the games you've chosen to remain accessible while in Family View.

In order to add and remove games from this list you first need to disable Family View:

1. Log into the account.
2. Select the **Family View** icon.
3. Enter your **Family View PIN** to exit Family View.

Then, you can authorize the game with one of two methods:

- Find the game in your Library and right-click on the game and click **Add to / Remove from Family Games**.
- Visit the **Family tab** within **Settings** and click **Family View** to run through the Family View wizard again. This will provide the option to add or remove games from your Family Games group. Once finished, to return to Family View select the **Family View** icon and confirm your choice.

Changing Family View options

To modify your Family View options:

1. First, log into the account.
2. Select the **Family View** icon.
3. Enter your **Family View PIN** to exit Family View.
4. Open the **Steam Settings** menu.
5. Go to the **Family** tab on the left side of the window that opens.
6. Click **Family View** to start the Family View wizard again.
7. Step through the Family View options wizard to select new content and features for Family Mode. You'll also be asked to select a PIN, which you're welcome to change or leave the same.

Disabling Family View

To remove Family View from your or your child's account:

1. Exit **Family View**.
2. Open the **Steam Settings** menu.
3. Go to the **Family** tab on the left side of the window that opens.
4. Select **Disable Family View** from the right side of the Family View window. Confirm your selection on the next window. Note: If using Big Picture, uncheck the box in the first page of the Family View wizard.

This will remove all restrictions from the account. If you wish to enable Family View in the future, simply revisit the "Family" tab in Settings and step through the Family View wizard once more. Your selected options will remain the same if you disable and re-enable the feature again in the future.



Roblox (Rated 7+, Multiplayer Online Game, World Building, Social Networking)

Roblox, first launched in 2005, has become and remains a very popular multiplayer online game for children 8 years old and up. It can best be described as Minecraft meets Fortnite. Roblox is free to play.

Once a player has signed up and created an avatar, they are given their own piece of real estate along with a virtual toolbox (known as "Roblox Studio") for building. They can monetize their creations to earn "Robux" (our virtual currency on Roblox), which can then be used to purchase more avatar accessories or additional abilities in one of the millions of experiences available on the platform. Roblox gives players a safe, comfortable place to play, chat, and collaborate on creative projects. If so inclined, they can even learn how to build and code experiences for others, all at their own pace.⁴

Since Roblox appeals to younger children, it is likely this game may be your child's first experience playing a multiplayer game. Roblox calls itself the "social platform for play." It's Roblox social media

features (i.e., Chatting) that causes parents so much anxiety. On March 2, 2017, Roblox added additional safety features that make it potentially one of the safest multiplayer game out there, provided parents take time to help their child set up their account and use the game's parental controls.

Problems: There has only been one real problem with Roblox is very young children playing it without parental controls or supervision. I have counseled several parents over the years that were devastated to find their child was being sexually exploited or groomed on Roblox. They did not know about the parental controls and they did not regularly check up on their activity.

Parental Controls:

Account Set up

When you register your child on Roblox, it is important to register their true age. Roblox has default security and privacy settings that vary based on the player's age. You can check the age range of your child's account in the upper-right corner of the navigation bar: **13+** or **<13**. If you check your child's account (maybe they set it up themselves), you can easily change the age in the account settings section.

Roblox uses filters that weeds out bad words and other problematic communication (e.g., phone numbers and addresses) for both <13 and 13+ accounts. When a user age 12 and under signs up on Roblox, they are automatically placed on controlled settings so that they can only directly message other users that are accepted as friends on Roblox. Players with 13+ accounts can see and say more words and phrases that <13 players. Links to YouTube videos and social media usernames can be shared by 13+ players.

All user-uploaded images are reviewed by human moderators for inappropriate content before it is posted. Although Roblox is rendered in a blocky Minescraftesque world, parents should be aware some user-created games on Roblox might include themes or imagery not appropriate for young players. You can restrict your child's access to a subset of curated games. You can find these settings in **Account Restrictions** under the **Security tab** in the **Settings** menu.

Chat Settings

Account owners have the ability to limit or disable who can chat with them, both in-app or in-game, who can send them messages, and who can follow them into games or invite them to private servers.

To changing the privacy settings:

1. Log into the account.
2. Go to account **Settings**.
3. Browser - find the icon located at the upper-right corner of the site.
4. Mobile Apps - find the three dots icon for **More**.
5. Select the **Privacy** tab.
6. Adjust the **Contact Settings** and **Other Settings**.

- Players age 12 and younger can select either **Friends** or **No one**. Players age 13 and older have additional options for privacy settings.

How to Block Another User

To block another user in the browser or mobile apps:

1. Visit the user's profile page.
2. Select the three dots in the upper right corner of the box containing their username and friends/followers information.
3. A menu will pop up, where you can select the option to **Block User**.

To block another user from inside a game follow the steps below:

1. Find the user in the leaderboard/player list on the upper-right of the game screen.
If the list is not visible, it is likely just closed. To reopen it, select your username in the upper-right corner. Note - the leaderboard may not appear if you are using a small-screened device such a phone, in which case you would need to use the profile page method outlined above.
2. Once you have found the name of the user you wish to block inside of the leaderboard, select it and a menu will open up.
3. Select **Block User**. You can also choose to Unblock them or Report Abuse directly from this menu as well. Once you have blocked the user, the icon to the left of their name will turn into a circle with a line through it to indicate they have been blocked.

Monitoring Account Activity

Roblox has several ways to monitor account activity. While logged in, you can view the following histories from their related sections:

- Direct and small group chat (**Chat** feature found in the lower right corner of the apps). There you can see individual chat histories. This feature is limited to Friends, and Friends of Friends.
- Private message history (**Messages**)
- Friends and Followers (**Friends**)
- Virtual item purchase and trade history (**My Transactions**, browser only)
- Creations such as games, items, sounds, ads...etc (**Create**, browser only)
- Recently played games (**Home**, **Keep Playing** or **My Recent**)

Recommendations: Safe for children aged 9-years and older with parental controls and active parental supervision.

Other Considerations and Things to Talk about with Your Child

- Make sure your child does not use their real name to sign up.
- Use a strong password and tell them never to share it with anyone.
- Log into the game via the app or website and then go to settings/account info and provide your parent email address. Make sure your child doesn't have access to your email account.
- When you have received Roblox's email to verify your email, follow the link and set a 4 digit PIN that only you know in settings/security. This prevents your child changing the restrictions.
- Enable Account Restrictions in Settings/Security.
- For extra security set Two-Factor Verification to prevent your child's account from being hacked.
- Turn off notifications in settings, if your child isn't going to be playing with friends online for extra security
- Make sure your child's social media accounts are not listed in the settings/Account info. If they are, make them private or remove them.
- Talk to your child about the dangers of revealing personal information to someone they meet online. Even if your child "knows" someone for a long time online, they should never tell a stranger their real name, nor chat or message them outside of the game.



Fortnite (Rated 12+, Multiplayer Online Game, Social Networking)

Fortnite is a video game for PlayStation 4, Xbox One, Nintendo Switch, Windows, Mac, and mobile that takes elements from sandbox-building games and adds the fast-paced action of a third-person shooter. There are two modes to the game: a solo version called Save the World and the hugely popular multiplayer version called Battle Royale.⁵

Problems: There are depictions of violence in game play. The violence is cartoonish and not particularly bloody or gory.

Players can spend real money on items in Fortnite. The game itself is free to play, so Fortnite encourages players to purchase items like weapons to be used in the game. There's also the Premium Battle Pass, a \$10 subscription that lets players compete on more levels and win exclusive game skins/costumes. Children have been bullied or ridiculed if they play with the free skin pack.

Fortnite has a live unmoderated chat. Consequently, the Fortnite chat environment can get very toxic. Fortnite chat also allows your child to talk to strangers that are playing in their game.

Parental Controls: Fortnite offers a range of parental controls to help you manage what a player can see and do in Fortnite. In addition to the controls within Fortnite, you can make adjustments through the Epic Games Store as well as your preferred gaming platform, including PlayStation, Xbox, Nintendo Switch, and mobile devices. The parental controls through the Epic Games Store and your preferred gaming platform include the option to restrict purchases.⁶

Parental Controls Within Fortnite

1. Launch Fortnite on your platform of choice.
2. Once in the Lobby, open the menu in the upper-right of the screen.
3. Select **Parental Controls**.
4. You will be asked to confirm the email address linked to the account. If no email address is linked to the account, you'll be guided to a web browser so that you may link one.
5. Set a unique six-digit PIN. This PIN will be required to change parental controls in the future, so make sure to set a PIN that is different from other PINs that you use and is easy for you to remember.
 - If you forgot your PIN or just want to change it, you can follow the steps in our support article on how to reset your PIN for parental controls.
6. Set the parental controls that you wish to have enabled or disabled.

SETTINGS OVERVIEW

Can See Mature Language - ON or OFF

- **ON:** Mature language can appear in text chat.
- **OFF:** Mature language in text chat will be filtered and replaced with heart symbols. (Recommended for under 12-years-old)

Can Accept Friend Requests - ON or OFF

- **ON:** Player receives all friend requests as normal.
- **OFF:** Player cannot receive friend requests. Incoming friend requests will be automatically denied. (Recommended for under 12-years-old)

Non-Squad Members Can See Your Name - ON or OFF

- **ON:** Players who are not in your squad will be able to see your display name.
- **OFF:** Replace your display name to players who are not in your squad with "Anonymous." (Recommended for under 12-years-old)

Can See Non-Squad Member Names - ON or OFF

- **ON:** You will see the display names of players who are not squad members. (Recommended)
- **OFF:** Replace the display names of players who are not in your squad with "Player."

Voice Chat - ON or OFF

NOTE: This setting only enables/disables Fortnite's in-game voice chat. The platform you are playing on may have additional communication features that must be restricted separately. Information on platform-specific controls can be found below or by clicking the "More Settings" button in-game.

- **ON:** You can hear your teammates and talk to them using a microphone.
- **OFF:** You cannot hear or talk to teammates. (Recommended for under 12-years-old)

Houseparty Video Chat in Fortnite - ON or OFF

Fortnite players who use the video chat app Houseparty can link their Houseparty and Epic accounts and have their Houseparty video chat shown alongside their Fortnite game. Houseparty video chat is currently available to Fortnite players on PC, PlayStation 5, and PlayStation 4.

NOTE: Because Houseparty is a separate application, this Fortnite parental controls setting does not control any features within the Houseparty app and does not prevent a Houseparty user from joining a room which is being shown in another player's Fortnite game.

NOTE: This setting cannot be enabled if Voice Chat is disabled through parental controls.

- **ON:** If they have linked their Houseparty and Epic account, a player can set their Houseparty video chat to show up on the same screen they are playing Fortnite on. While in use, Houseparty friends and friends-of-friends can be seen and heard while playing Fortnite.
- **OFF:** The player is not able to set their Houseparty video chat to show up on the screen they are playing Fortnite on (this will not affect the player's ability to use Houseparty outside of Fortnite). (Recommended)

Weekly Playtime Reports - ON or OFF

NOTE: Click on the **More Settings** button in-game to learn about playtime restrictions for your platform.

- **ON:** A weekly playtime report will be sent to the email address associated with the account. (Recommended)
- **OFF:** No playtime reports will be sent.

Text Chat - ON or OFF

NOTE: This setting only enables/disables Fortnite's in-game text chat. The platform you are playing on may have additional communication features that must be restricted separately. Information on platform-specific controls can be found below or by clicking the "More Settings" button in-game.

- **ON:** You can send and receive text chat messages with your teammates.
- **OFF:** You cannot send or receive text chat messages with your teammates. (Recommended for

under 12-years-old)

Use the **SAVE** button to save your selections. If you wish to change any of these settings in the future or disable parental controls, you will need to enter your PIN. The email associated with the account will be notified whenever a PIN is changed.

Parental Controls Via Gaming Platform

The parental controls within Fortnite only apply to the features in Fortnite, regardless of the platform that it's being played on. This means that if you, for example, turn off voice chat in Fortnite, you may still be able to access voice chat for the game using communication methods outside of it, such as by using the party system built into your console.

If you would like to more broadly restrict access to such features, you can do so at the platform level on PlayStation, Xbox, Nintendo Switch, Windows 10, iOS, and Google Play. This includes restricting access to purchases. See the following chapters on parental controls on PlayStation, Xbox, Nintendo Switch, Windows 10, iOS, and Google Play.

Epic Games Store Parental Controls for Fortnite

On the Epic Games website, you have access to parental controls for the Epic Games Store. These controls offer you the ability to use a PIN to restrict Epic Games Store purchases (as well as to restrict access to content on the Store based on age ratings). Epic Games Store purchases include in-game Fortnite purchases made through the Epic Games Store (purchases on PC, Mac, the Epic Games App on Android, and iOS and Google Play through Epic direct payment).

NOTE: Purchases made through the Epic Games Store do NOT include in-game Fortnite purchases made through PlayStation, Xbox, Nintendo, the Apple App Store, or the Google Play Store. For info on parental controls for these, please refer to the “Parental Controls via Gaming Platform” section above.

There are two paths to open the Epic Games account settings to adjust parental controls:

Directly from epicgames.com

1. Go to epicgames.com.
2. Log in at the top right.
3. Hover over your account name.
4. Select **Account** to go to your account settings.

From the Epic Games Store Launcher on PC/Mac

1. Open the Epic Games Launcher and log in.
2. Click on your account name in the bottom-left corner.
3. Select the **Manage Account** option. This will open a web browser with your account settings.

Now that you're in the account settings, scroll down to the **Parental Controls** section in the General Settings page.

From here, you can set or enter your six-digit PIN.

- This PIN will be required to change parental controls in the future, so make sure to set a PIN that is different from other PINs that you use and is easy for you to remember. If you already have a PIN for Fortnite, your PIN # will carry over.
- If you forgot your PIN or just want to change it.

Epic Games Store parental controls include:

- Changing your PIN.
- Requiring a PIN for Epic Games Store purchases.
- Limiting access to games based on their ESRB, PEGI, or GRAG age rating.

When you're done setting your options for parental controls, save them before closing the options window. To turn parental controls off, select **Turn Parental Controls Off** in the Parental Controls section of the General Settings page and input your PIN.



Minecraft (Rated 9+, Multiplayer Online Game, World Building, Social Networking)

Minecraft is a sandbox-adventure video game. The style is called "sandbox" because it provides a creative landscape with no fixed goal and endless possibilities. Minecraft doesn't come with instructions, and it's relatively simple to pick up and play. The more you play, the more you learn what to do and how to use the available resources, such as redstone and different kinds of ore, to make ever-more-complex tools and structures.⁷

Problems: Like Roblox, there has only been one real problem with Minecraft, very young children playing it without parental controls or supervision. All multiplayer online games offer the possibility of your child meeting a predator or being the target of bullying. Thankfully, Minecraft does have filters and removed some problematic features that made Minecraft more dangerous in the early days..

Parental Controls: There are no in-game parental controls, but Microsoft has added some new features to make Minecraft more safe for your child. Minecraft has chat filters that screen out profanity, email addresses, phone numbers, and ages. Private messaging is no longer part of Minecraft multiplayer either. Minecraft also has in-game reporting of inappropriate behavior.

Of course, playing in single-player mode is the safest choice, but sooner-or-later, your child will want to play with their friends on a server. A server is a software setup that lets players organize and host multiplayer games. Anyone can set up a server, but it's a little technical. Some parent groups set up a server just for children and friends. Playing on a reputable server will also help keep your child safe. Family safe servers that partner with Minecraft have teams of moderators that ensure everyone is getting along, and that the chat filter is doing its job. Most servers also have expanded chat filters. For example, Autcraft is a Minecraft server designed just for kids on the autism spectrum, and Famcraft is a server that's family friendly.

Xbox Live Parental Controls for Minecraft

If your child is playing Minecraft on Xbox, you can set privacy and multiplayer preferences:

1. Log in to your Xbox Live Account at xbox.com. If you don't have a Xbox Live Account, you can create one for free, but you have to sign up using a Microsoft account.
2. Once in your Xbox Live Account, click on your username in the top right corner of the browser's window and click **Xbox Profile**.
3. Click on **Privacy Settings**.
4. There are a number of settings here with the choice of Everyone, Friends, or Block. We recommend at a minimum chose **Friends**, and for the most restrictive setting, choose **Block**.

My Child Wants an App Not Discussed in this Book. What Do I Do?

Apps, like technology, are always changing. Some apps like Instagram or Snapchat will be around for a long time, but there will always be new apps that pop up and create problems for our kids. To stay on top of current apps and how they might impact your child, join my e-newsletter and read my published articles at cybersafetycop.com. You can also follow me on Facebook, Twitter, and Instagram.

Social Media Apps Appropriate for Elementary Aged Children

A lot of parents are asking for safe social media app recommendations for their elementary-aged children. Although no social media app is entirely secure, there are a few notable apps created with younger children and their parents in mind. Excessive screen time on these apps can still be a problem, so limit use.



Village-Safe Social for Family (Rated 4+, village.me)

Village-Safe Social for Family is intended to be used by the whole family and has extensive parental controls. There are no "likes" or "followers." Parents have complete control over who their child is interacting with. Messages, or hyperlinks in the messages, can be quickly flagged as inappropriate. Image recognition software will blur and block images it determines to be problematic in the app's messaging feature.



Messenger Kids (Rated 4+, messengerkids.com)

Messenger Kids is owned by Facebook and has included face filters, which kids like to use and share with friends. It is a well-known name among children, so it is likely that kids naturally chose it to communicate with their friends. The parental controls are excellent, giving parents the ability to control who can interact with their child. Lastly, message history cannot be deleted, giving parents the ability to review what is being sent and received.



Kinzoo Messenger for Families (Rated 4+, kinzoo.com)

Kinzoo Messenger is similar to Village Social. There are no "likes" or "followers." Parents have control over who their interacts with. It is a messaging app designed aesthetically for young children. Tweens might find it unappealing for being too little kid like.

iPhone & iPad Parental Controls

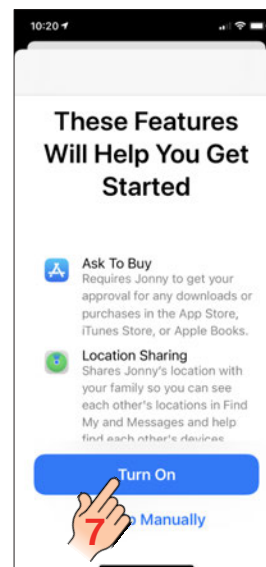
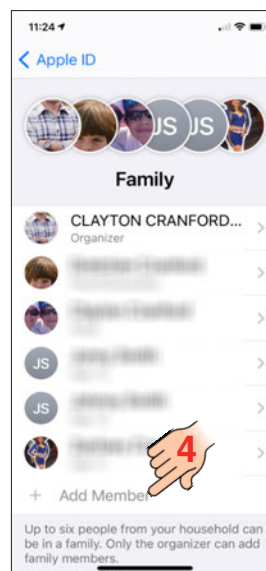
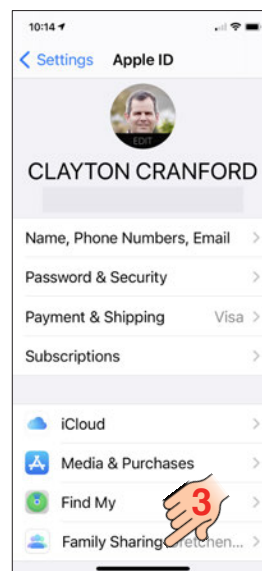
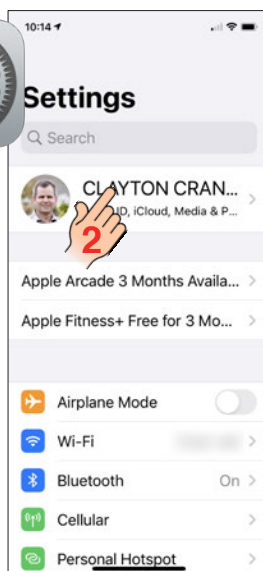
Parental Controls and Screen Time works via Family Sharing, so as long as your children are part of your Family in the Family Sharing settings, you'll be able to view and control their Screen Time options from your phone. If the child has an iPhone, and the parent has an Android phone, Screen Time settings can be set on the child's device. Unfortunately, the parent will have to access the child's phone to see screen time information or make changes to the settings. The best situation is for the parent and child to both have iPhones and connected with Family Sharing.

Step 1: Setup Family Share

1. Select **Settings** from your home screen.
2. Select your **Apple ID** at the top of the screen
3. Select on **Family Sharing**
4. Select **Add Member**
5. Select **Create an Account for a Child**
6. Select **Continue** and enter your child's name and date of birth.

Note: You cannot exert parental controls or screen time on anyone 18-years-old or older.

7. Select **Turn On Ask to Buy and Location Sharing**



Step 2: Setup Screen Time

1. Return to the Settings screen and select **Screen Time**.
2. Select your child's account.
3. Select **Turn on Screen Time**

Setup Downtime

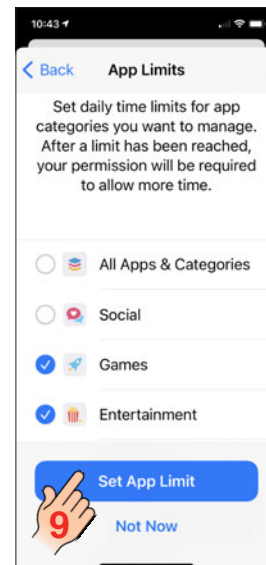
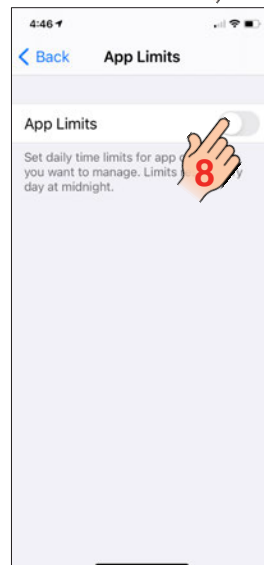
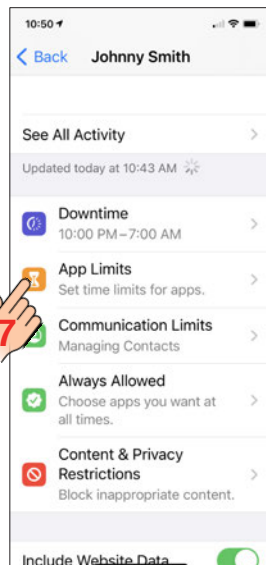
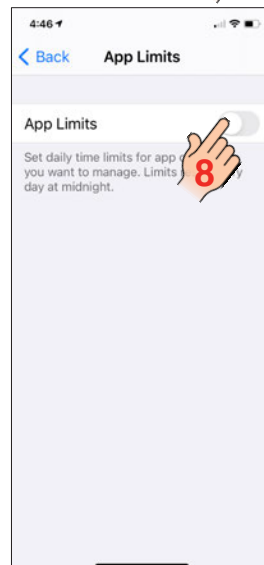
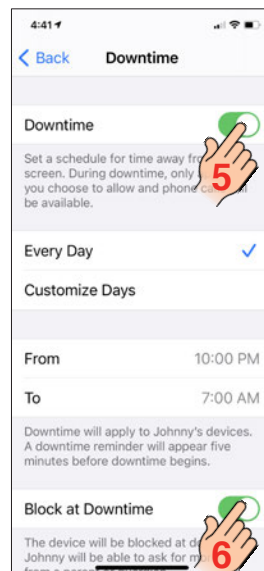
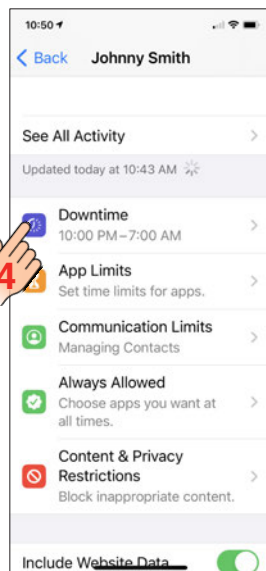
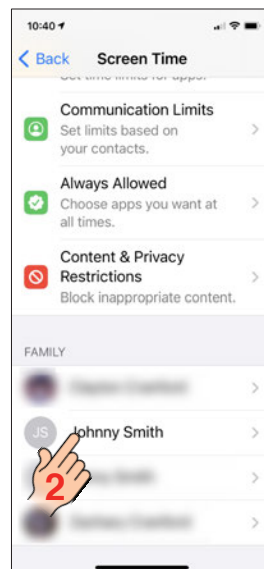
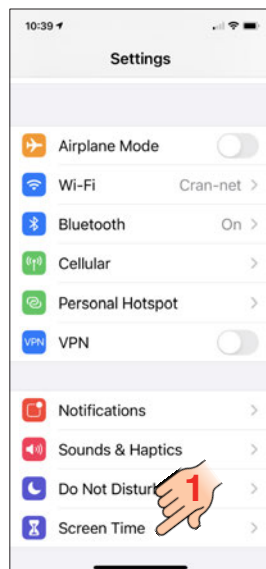
When downtime is active, only phone calls and apps that you choose to allow are available. Downtime applies to all of your Screen Time-enabled devices, and you get a reminder five minutes before it starts.

4. Select **Downtime**
5. Turn on **Downtime** and choose Every Day or Customize Days and the time.
6. Select **Block at Downtime**.

Setup App Limits

You can set daily limits for app categories with App Limits.

7. Select **App Limits**.
8. Turn on App Limits
9. Choose the categories of apps you want to limit, the max amount of time, and then select **Set App Limit**.



Setup Communication Limits

Control who your children can communicate with — throughout the day and during downtime.

10. Return to Screen Time settings and select **Communication Limits**.

11. Select **Manage [your child's] Contacts**. You can add contacts from your list of contacts or add new ones here.

12. Select **During Screen Time** to limit phone class, FaceTime, Messages, and iCloud contacts.

13. Select **During Downtime** to limit phone calls, FaceTime, Messages, and iCloud contacts.

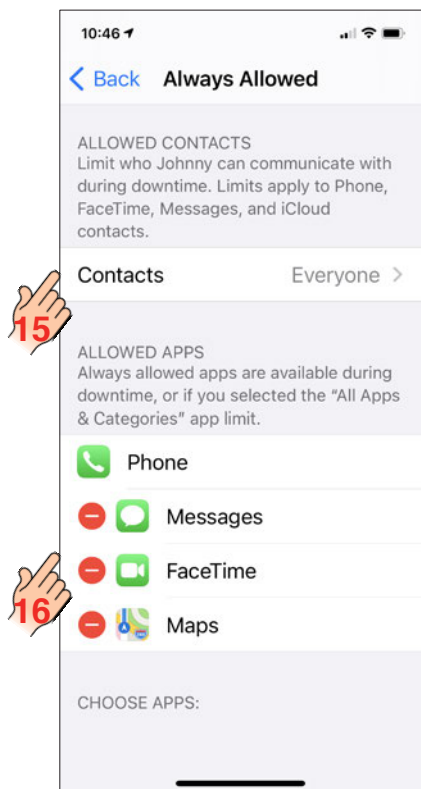
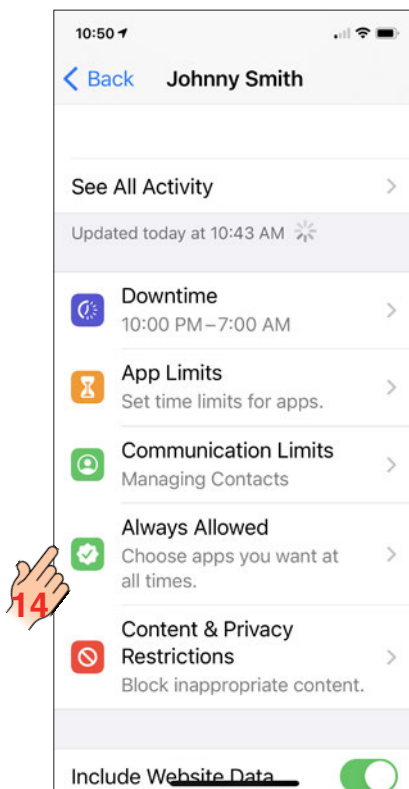
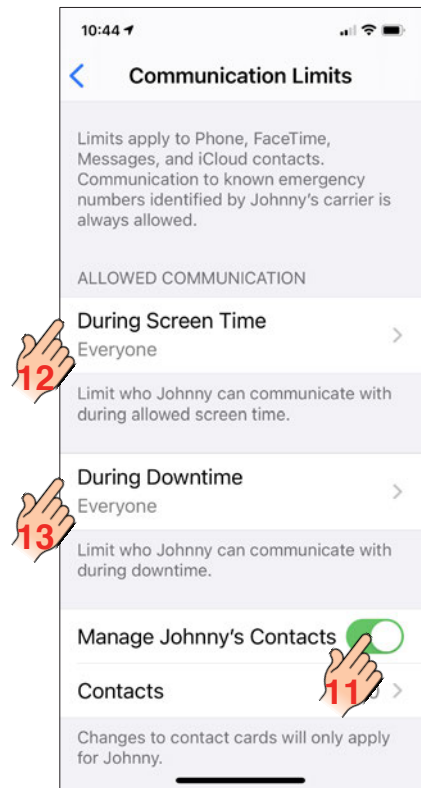
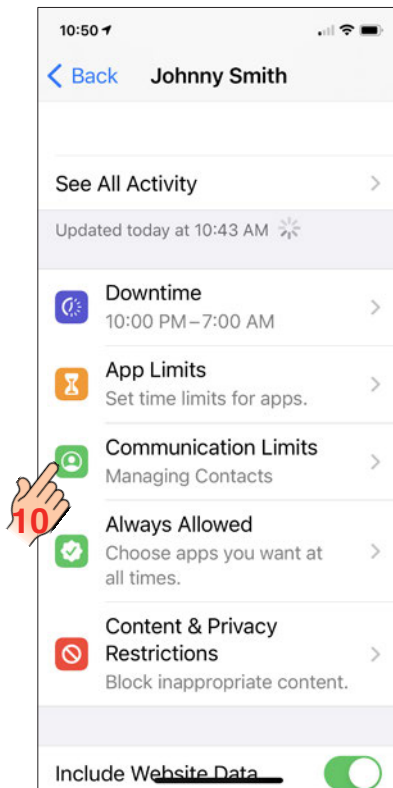
Setup Always Allowed

These apps and contacts will always be available during Downtime.

14. Select **Always Allowed**.

15. Select **Contacts** to define who your child can communicate with during Downtime

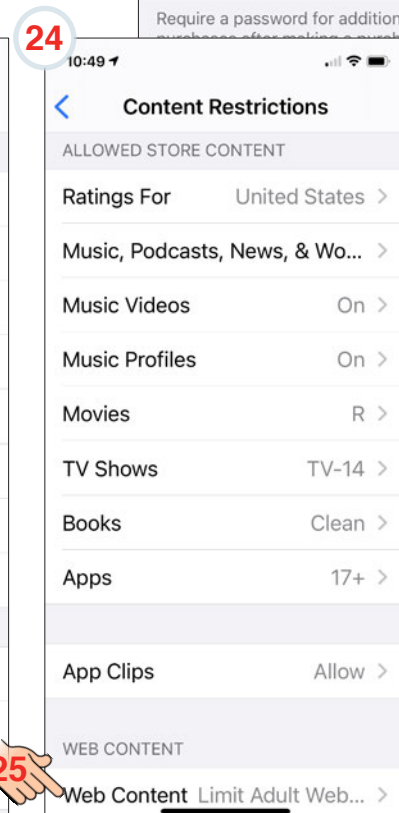
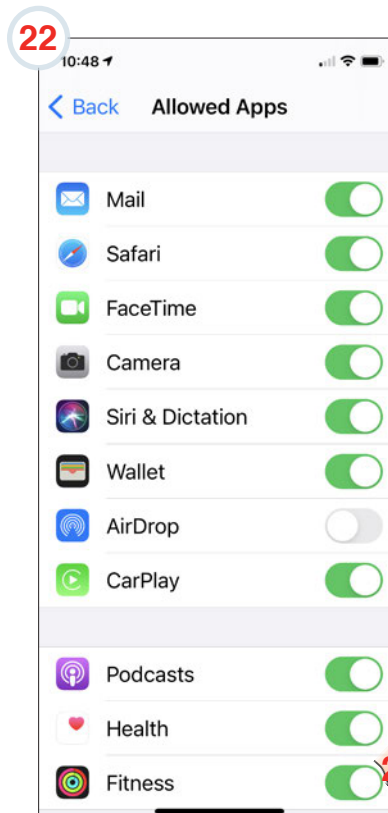
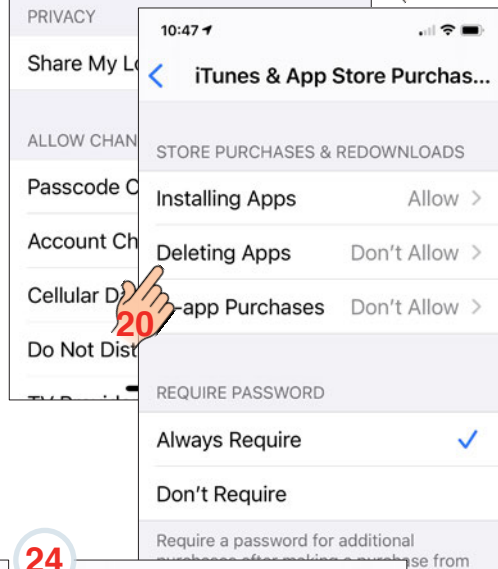
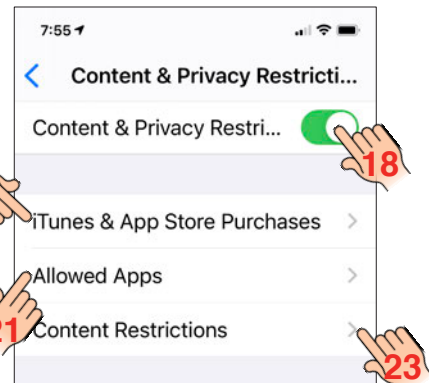
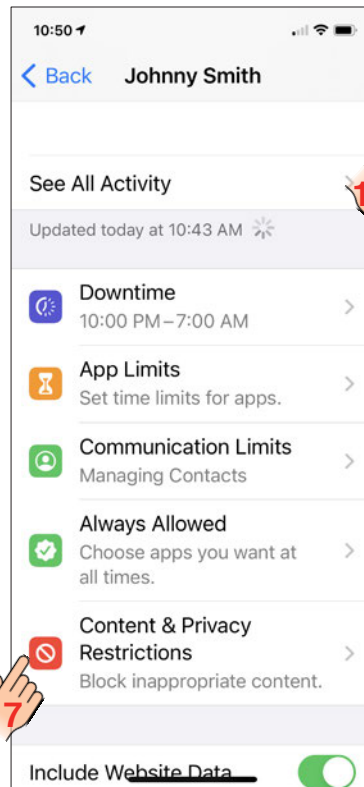
16. Remove apps that you don't want access to during Downtime.



Setup Content & Privacy Restrictions

You decide the type of content that appears on your child's device. Block inappropriate content, purchases, and downloads, and set the privacy settings.

17. Return to Screen Time settings and select **Content & Privacy Restrictions**.
18. Turn on **Content & Privacy Restrictions**.
19. Select **iTunes & App Store Purchases**.
20. Don't Allow **deleting apps** or **in-app purchases**. Always require a Password.
21. Select **Allowed Apps**.
22. Turn off apps you do not want your child accessing. Turn off **AirDrop** at a minimum to prevent someone from sending an unsolicited explicit image.
23. Select **Content Restrictions**.
24. Set the content restrictions based on what you think is most appropriate for your child.
25. Select **Web Content** restrictions.

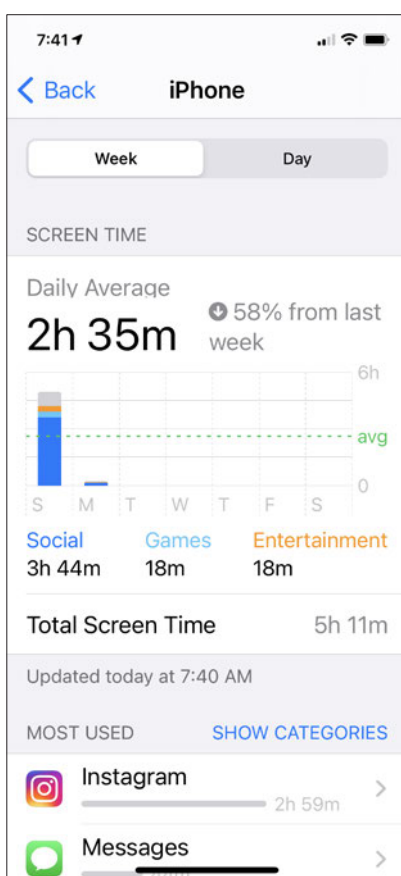
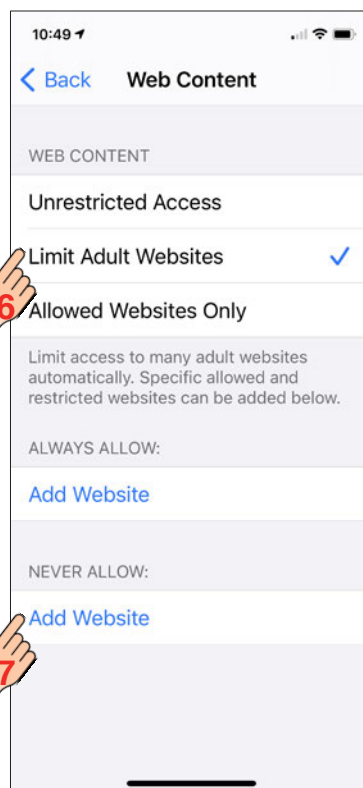


26. Select **Limit Adult Websites**. When Limit Adult Websites is enabled, your child cannot delete Safari's search history.

27. Add **Websites** that you want to block from your child's Safari Browser. Suggested sites to include:

- Imgur.com
- Reddit.com
- Baidu.com
- Yandex.com
- Dogpile.com
- Flickr.com
- Liveleak.com
- Excite.com
- Instagram.com
- Tumblr.com
- Twitter.com
- Omegle.com
- <https://www.youtube.com> (if you want to completely limit YouTube access)

28. Don't Allow **Passcode changes** or **Account Changes**. If you do not do this last step, your child can delete your parent notification app and change the Screen Time settings.



The **Screen Time Report** shows you how your child uses their device. You can use this information to help you make decisions about managing the time your child spends on their devices. A description of the device's use includes:

How much time spent using apps by category, a breakdown of your app use by time of day, an overview of the types of notifications you get, and how often you pick up your device and which apps you use. You can tap each app in your Screen Time summary to see more information about its use.

How Children are Hacking iOS Screen Time



Parental controls are not the panacea we would like them to be. With enough time and Googling, your child will find a way to get around the parental controls you have set up. I have had more than a few parents reach out to me completely perplexed how their child can be on YouTube after their screen time has run out or after the parent thought they completely blocked it in the settings.

Think of parental controls like guard rails on the road. They are most helpful when you are driving up a twisty road on a mountainside. They are there to keep you on the road if something goes wrong. Could you drive in a way to blow through the guard rails? Absolutely. But, you don't because you know what's on the other side of the rail - a fatal drop. Your child has no idea what's on the other side of the guard rail. They will drive their car as fast as possible because it feels fun, safe, and inconsequential (underdeveloped prefrontal cortex). Acknowledging that our children will naturally push the limits of the parental controls and perhaps try to defeat them, we need to start with a talk.

Tell your child you know they are smart, and there are probably ways they can get around screen time limits or web filtering. Explain the parental controls are there to keep them safe. Use the guard rail metaphor if you like. Explain this is not a game or a challenge to defeat the parental controls. If they do, they will have violated the agreement to use their device (whatever it is), and there will be consequences. Be very clear about what your expectations are. Be equally clear about what the consequences will be. Hopefully, after this talk, you won't have to play detective to discover if your child is trying to hack the parental controls. Either way, you should periodically check-up with your child and make sure they are following the rules.

The following are some of the ways children are circumventing parental controls, how to recognize if they are doing it and how to stop them:

Changing Time Zones

If a child's favorite app is blocked during Downtime, they would typically have to request their parents for an extended time. However, before Downtime begins, it is possible to change the phone's time zone to extend their free time. To prevent this, you must make some adjustments on your child's phone:

1. On your **child's phone**, select **Settings > Screen Time >** scroll to the bottom of the screen and **Turn Off Screen Time**.
2. Go back to **Settings > General > Date & Time >** turn on **Set Automatically**.
3. Go back to **Screen Time** and **Turn on Screen Time**. Select **Use Screen Time Passcode**.
4. Select **Content & Privacy Restrictions** and toggle it on at the top of the screen.
5. Scroll down and select **Location Services**.
6. Scroll to the bottom and select **System Services**.

7. Untoggle **Setting Time Zone** (greyed out). Tap **< Back**.

8. At the top of the screen, check **Don't Allow Changes**.

App Limits Don't Seem to be Working

If your child is still playing away on their gaming app after they should have reached their limit, you may not have secured it on their phone.

1. On your **child's phone**, select **Settings > Screen Time > Add Limit**.
2. Choose the app categories and the apps you want to limit. Tap **Next**.
3. Set your time limit. IMPORTANT: Toggle on **Block at End of Limit**.

Watching YouTube after blocking it in Parental Controls

Make sure you have the full URL in the Web Content filter.

1. From **your phone**, **Settings > Screen Time > Content & Privacy Restrictions > Content Restrictions > enter passcode > Web Content**.
2. Select **Limit Adult Websites**.
3. Under NEVER ALLOW, add **https://www.youtube.com** (if you don't put it in exactly as shown, it will not block YouTube).

There is one more workaround to watch YouTube after it has been blocked by App Limits or Downtime. YouTube videos can be viewed through the Messages widget. You can remove the YouTube widget from Messages, but it can be added back. The only way to keep this from happening is by removing Messages from the Allowed List.

1. **Screen Time > Always Allowed > remove it from Allowed Apps** by tapping the red circle with the white minus sign.

Sending Text Messages via Siri

Perhaps you have Messages blocked during Downtime or after your child has reached their Time Limit, but they are still sending text messages. Siri may be their unwitting accomplice. Follow these steps to remove Siri as an Allowed App:

1. From your **child's phone**, select **Settings** from the home screen **> Screen Time > Content & Privacy Restrictions > enter passcode**.
2. Select **Allowed Apps**, toggle off **Siri & Dictation**.

Sending Text Messages via the Contacts app

Your child can get around the Messages app limit by going to the Contacts app, share the contact via Messages, and Messages come back up. To prevent this, you must turn off the Contact app:

1. From your **child's phone**, select **Settings** from the home screen **> Screen Time > App Limits >**

enter passcode.

2. Select **Productivity** and then the **Contacts** app. Select **Next**.
3. On the next page, give the Contacts app a short time limit, like 1-minute.
4. If you go back to the home screen, the app should be greyed out after 1 minute.

Sending Text Messages from a Messages Notification

If you swipe down to reveal the notifications panel and tap on a previous Messages notification, it will bring up Messages, and then you can send a text. To prevent this, you must open your child's iPhone notifications panel and clear out any messages notification after they have reached their Time Limit.

Deleting and Reinstalling Apps

Once an app's time limit has been reached, your child can delete the app, reinstall it from the app store, and then continue using it. To prevent it, follow the steps below:

1. From **your phone**, **Settings > Screen Time > Content & Privacy Restrictions > iTunes & App Store Purchases > enter passcode.**
2. Select **Don't Allow** for Deleting Apps.

Factory Reset

A factory reset is a desperate move, but it would erase all existing restrictions. The only problem is they will also erase all their data and essentially be setting up a new iPhone. Your child could back up their data on the family iCloud account linked to their phone and retrieve their data. This hack would only be possible if they had access to the iCloud credentials. Prevent this by keeping the iCloud password safe. If you notice no usage or abnormally low usage on their screen time tracking, then perhaps your child has reset their phone.



Android Parental Controls

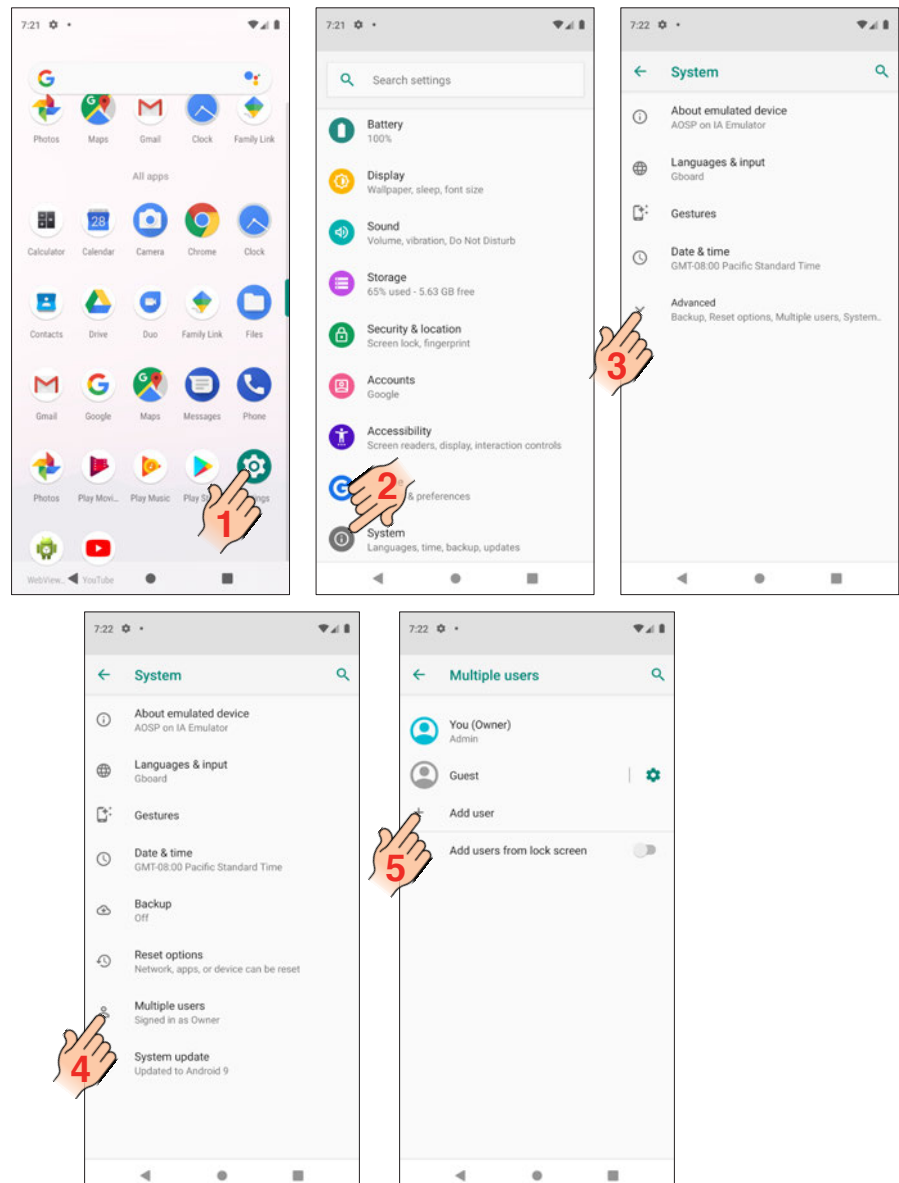
To set up parental controls on an android device for your child, you will need to first create an account for them. You have the option of creating a separate user on your Android phone or tablet, or creating a new user on a different device. Creating a separate user on your Android device might be a good choice if your child is not ready for their own device and you want to control their usage better.

Creating an account for your child

Creating a new user on your device.

1. Open your device's Settings app.
2. Tap System
3. Select Advanced
4. Multiple users. If you can't find this setting, try searching your Settings app for users.
5. Tap Add user.

The Users option has been removed on some devices (by device manufacturers who also tweak Android). In some instances, it will be buried in the Accounts or System section of the OS. If you're struggling to find it, then Google your specific phone model and "add child account."



Creating a new user on a new device

1. Turn on the new device and follow the instructions on screen to set up the device.
2. When you're asked to sign in with your Google Account, tap **Create new account**. If you don't see "Create new account," tap **More options** first.
3. Enter your child's name, birthday, gender, email address, and password.
4. Follow the instructions to sign in with your own Google Account, provide parental consent, and pick your child's settings.

Setting up parental controls with Family Link



If your child already has their own Google Account, you can add supervision and manage their parental controls with Family Link.

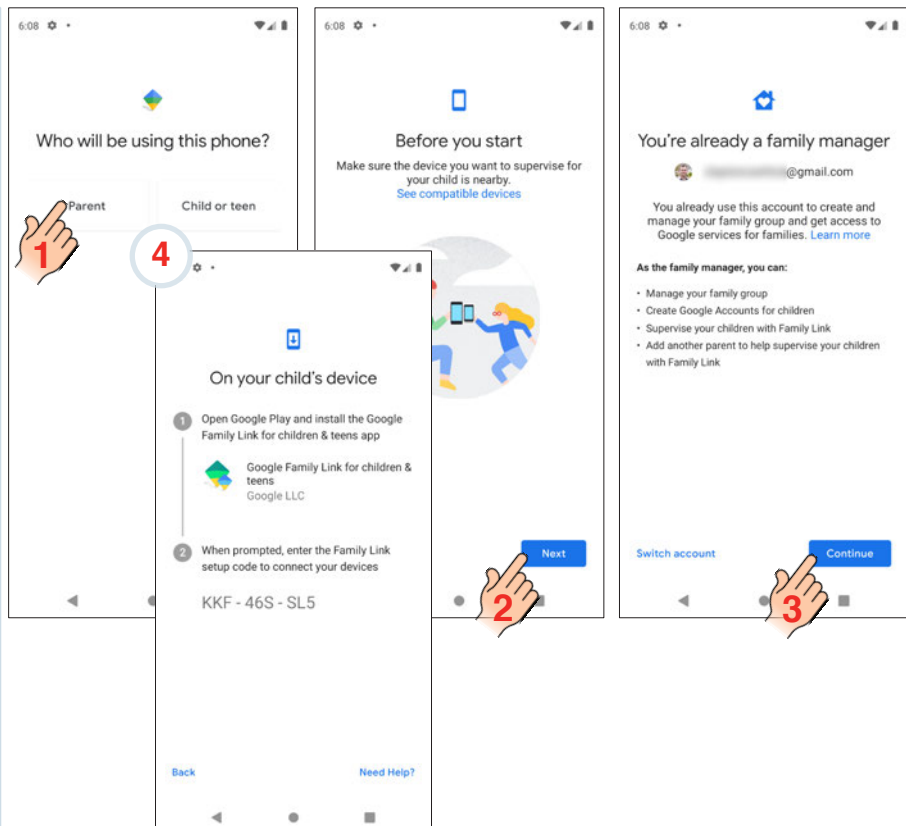
If your child under 13 (or the applicable age in your country) doesn't have a Google Account yet, you can create one for them and manage it with Family Link.

If you add parental supervision to your child's existing Google Account and your child is above the applicable age in your country, you or your child can stop supervision at any time. If your child stops supervision, you'll be notified, and your child's supervised devices will be locked temporarily.

You will need to download the **Google Family Link app** on the parent's device and the **Google Family Link for children & teens app** on the child's device. These are two different apps.

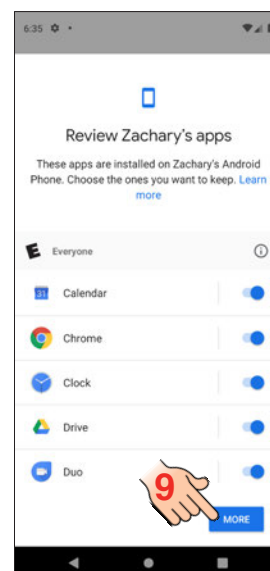
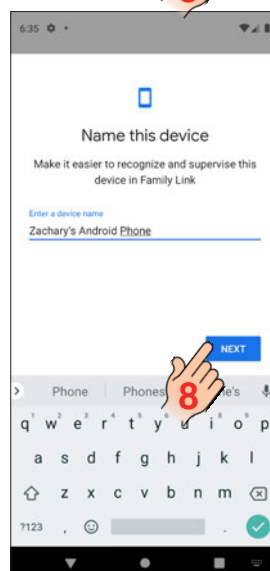
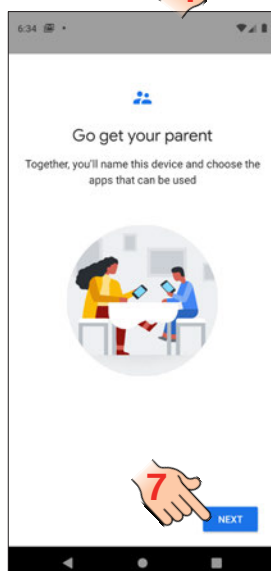
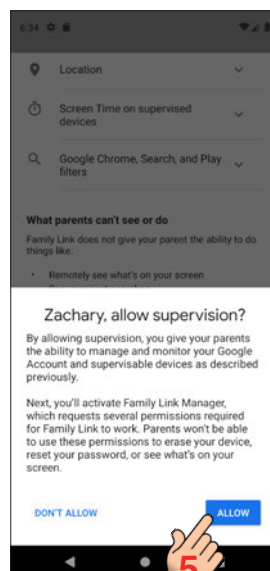
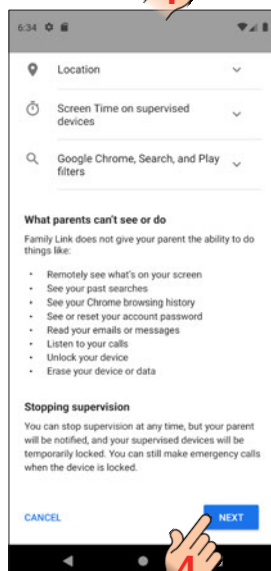
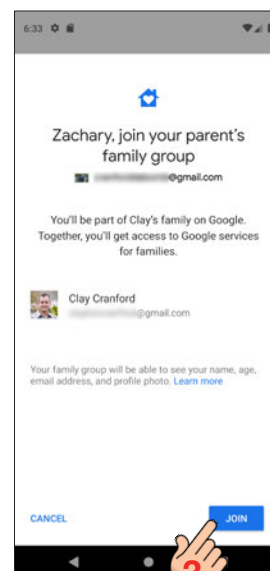
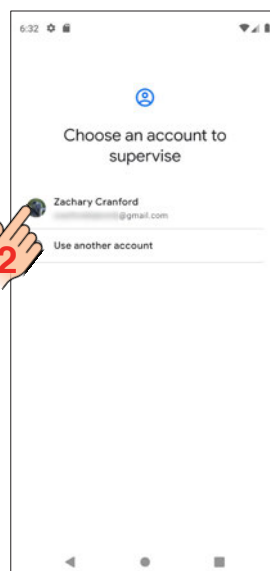
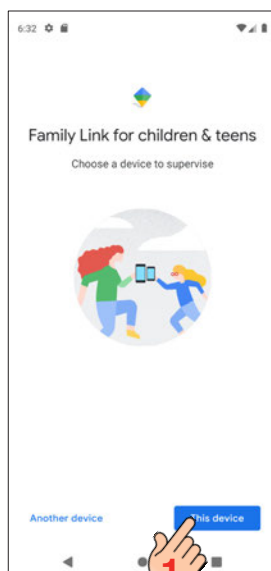
On the parent's device

1. Open the Family Link app on the parent's device and select **Parent**.
2. Select **Next**
3. Choose your account that will be managing the family's devices.
 - If your child already has a Google account (an email ending in @gmail.com) choose **Yes**. If they don't, create one and return here.
4. Get your child's device and open the Family Link for children app.



On the child's device

1. Open the Family Link for children & teens app and select **This Device**.
2. Choose your child's account that will be managed. **Next**.
 - Enter the 9-digit setup code from the parent's device.
 - Enter your child's Google account password.
3. Select **Join**.
4. At the bottom of the screen, select **Next**.
5. Select **Allow**.
6. Select **Activate this device admin app**.
7. Select **Next**.
8. Name your child's device
9. Switch off any apps you do not want your child using. Select **More** to see more apps. When you are done, select **Next**.
10. Finish following the final prompts and your child's device is ready to be managed from the parent's device.



Setting up the filters and controls.

1. On the parent's device, Select **Customize parental controls**, **Next**, and then **Continue**.

2. Select **Manage Settings**.

Setup Google Play Store

If you're a parent in a family group, you can require family members to get your permission for purchasing or downloading content on Google Play.

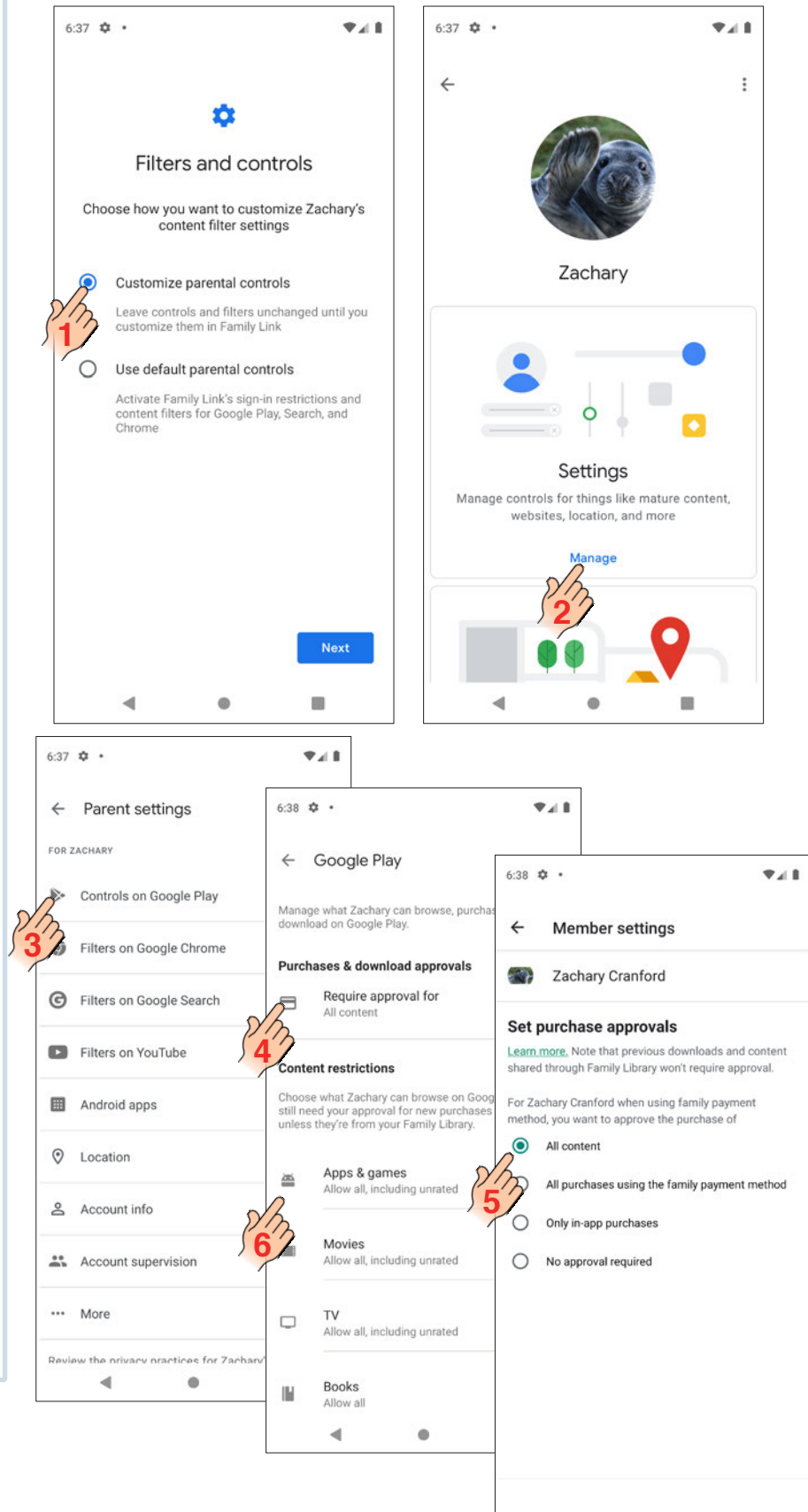
3. Select Controls on Google Play.

4. Select **Require approval for**.

5. Select **All content**.

Note: Previous downloads, updates, and content shared through Family Library won't require your approval, even if that content was acquired before supervised members are added to your family.

6. Set content restrictions on your child's Apps & Games, Movies, TV, Books, and Music. Tap on each category and set the appropriate level for your child.



Setup filters on Chrome

7. Select **Filters on Google Chrome**.

- Children won't have access to apps and extensions from Chrome Web Store.
- Children can't use incognito mode.

8. Select Try to block mature sites (sexually explicit and violent sites). This is not 100% effective. Or, select Allow only certain sites (your child will only be able to visit the sites you allow).

Filter explicit search results with SafeSearch

By default, SafeSearch is turned on for your child's account when you set up supervision with Family Link. SafeSearch helps filter explicit search results like pornography on Google Search. SafeSearch isn't 100% accurate but it helps children avoid most sexually explicit content while they use Google Search.

9. Select **Filters on Google Search**.

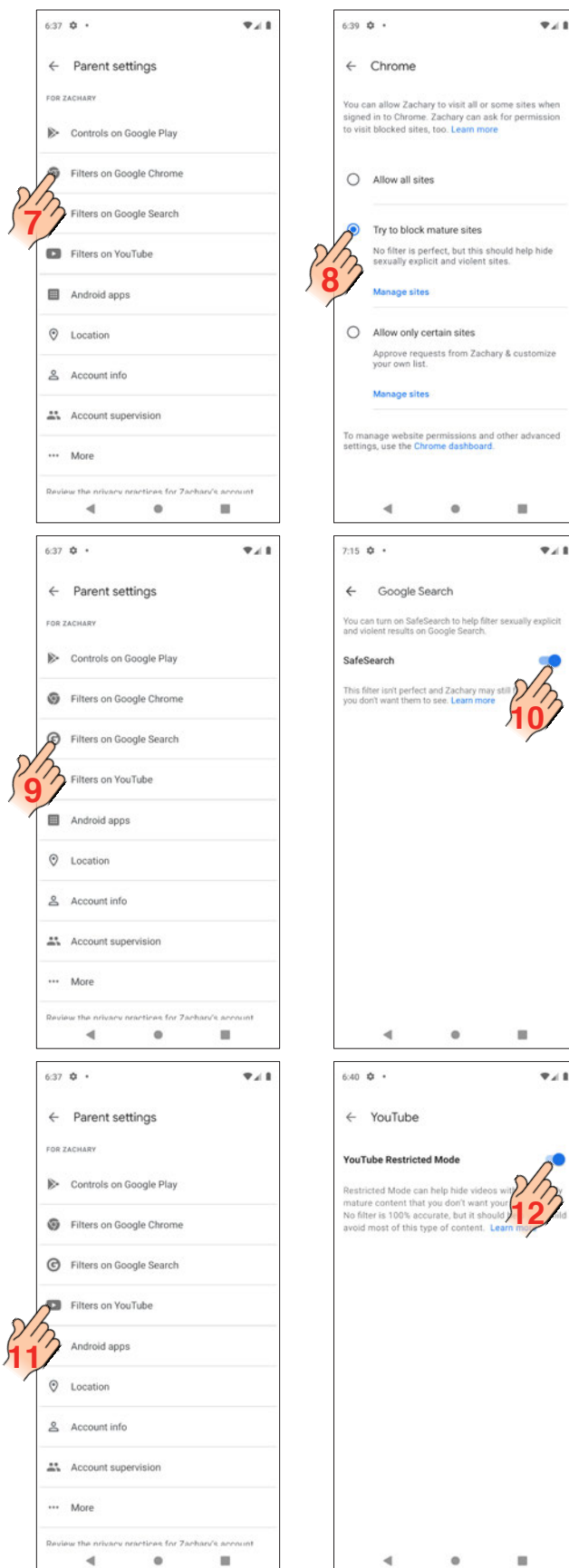
10. Toggle on **SafeSearch**

Enable YouTube's Restricted Mode

Restricted Mode is an optional setting that you can use on YouTube to help screen out potentially mature content that you may prefer your child not see. Restricted Mode uses video title, description, metadata, Community Guidelines reviews, and age-restrictions to identify and filter out mature content. It is not 100% effective. When restricted mode is enabled, you will not be able to see comments on the videos you watch.

11. Select **Filters on YouTube**.

12. Toggle on **YouTube Restricted Mode**



Manage Apps

13. Select **Android Apps**.
14. Select app of your choosing.
15. Toggle app on or off, or select Permissions.
16. Toggle settings on or off as desired.

Find & manage your child's Android device location

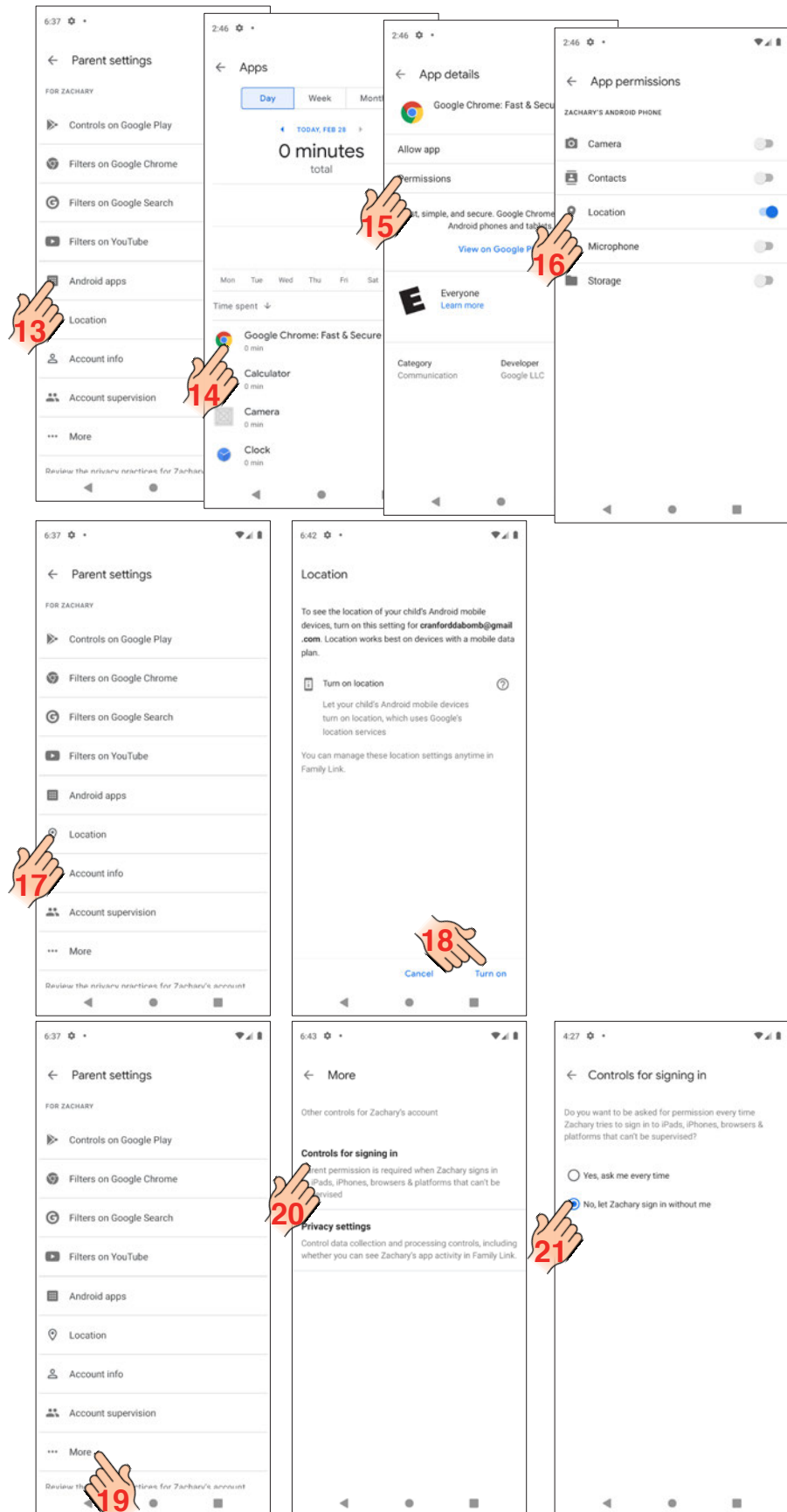
17. Select **Location**.
18. Select **Turn on**.

Note: You won't see your child's location in the Family Link app if:

- Their device is powered off
- Their device isn't connected to the Internet
- The device hasn't been used recently

Controls for signing in to other devices

19. Select **More**
20. Select **Controls for signing in**
21. Choose if you want to approve every time your child attempts to sign into a device that cannot be supervised.



Manage your child's screen time

When your child reaches the set a limit for their screen time, they'll get a notification when and their device will lock. When the device is locked, your child:

- Can't see notifications.
- Can't unlock the device or use any apps - except for apps designated as Always allowed apps.
- Can answer phone calls, and tap Emergency to make a call if the device has a calling plan (Android phones only).

22. On the "Daily limit" card, tap **Set up** or **Edit limits** and follow the on-screen instructions.



23. Toggle on **Scheduled**, and then select each day you want to limit screen time and the maximum amount of hours of usage for each day.

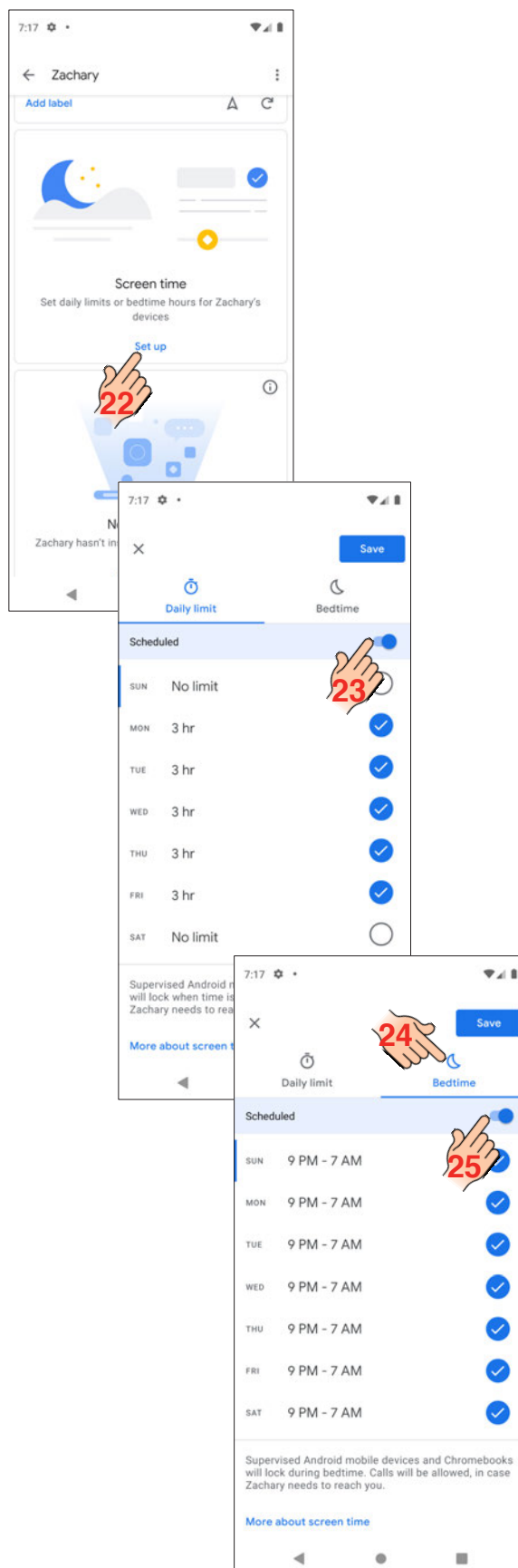
24. Set bedtime, when you child's device will not function, by selecting Bedtime.

25. Toggle on **Scheduled**, and then the bedtime for each day.

How to give your child bonus time

You can let your child spend more time on their device for the day without changing their daily limit or bedtime schedule.

- Open the Family Link app and select your child.
- On the card for one of your child's Android or Chromebook devices, the Bonus time chip  will appear when your child's device is locking soon or if your child's device has already locked.
- Tap  and follow the instructions on the screen to give your child bonus time for the day.



Limit screen time for specific apps

You can set time limits on apps to manage how much time your child can spend on a specific app each day.

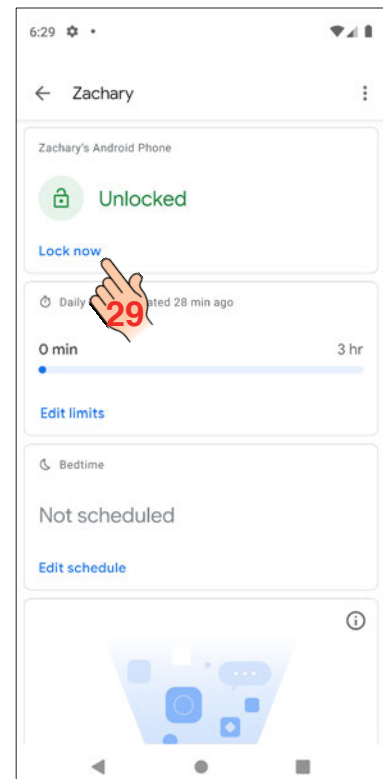
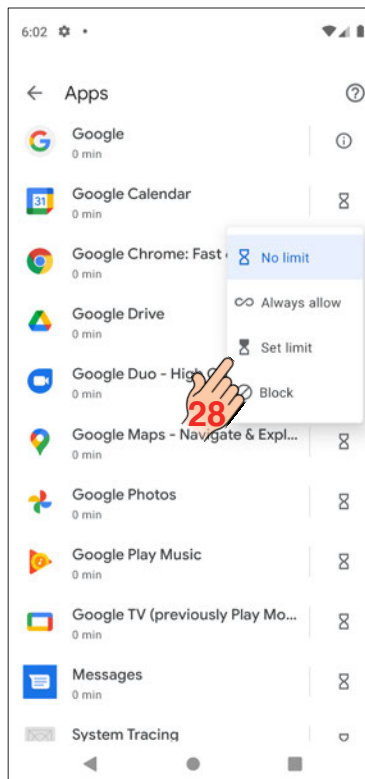
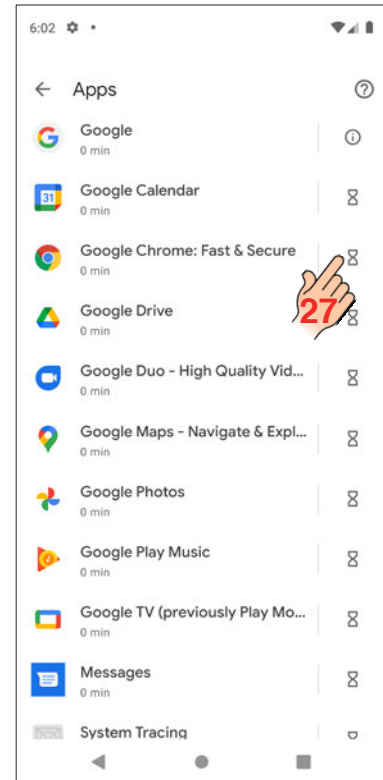
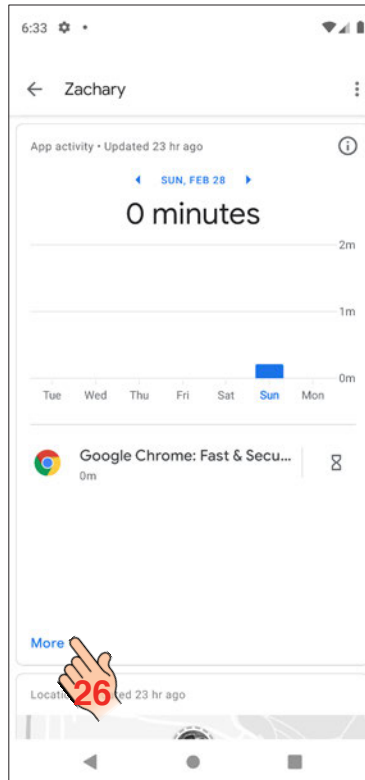
26. On the "App activity" card, tap **Set limits** or **More**.
27. Next to your desired app, tap Empty hourglass and then Set limit Set limit.
28. Set a daily time limit for the app or block it completely.

Note: Always allowed apps don't count toward your child's screen time limits and aren't available after bedtime.

If parents tap "Lock now," Always allowed apps aren't available, unless you change this setting from the device lock card.

Lock your child's device

29. On the card for one of your child's Android devices, tap Lock now or Unlock.





Xbox Parental Controls



The Xbox Family Settings app (iPhone and Android) will enable parents to apply settings for gaming activities on Xbox Series X|S and Xbox One. Content and screen time limits can be applied to

Windows 10 PCs when a child account is logged into the Microsoft account with Xbox profile that is part of your family group.

Add a child that has a Microsoft account

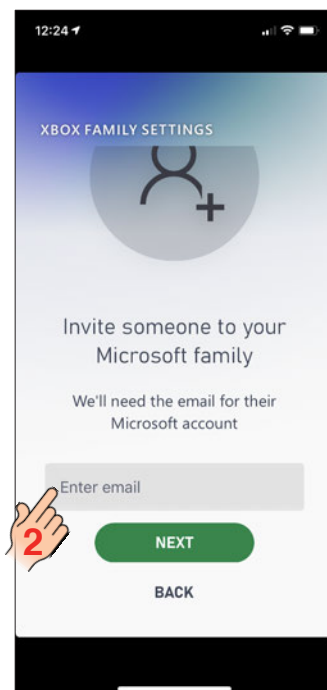
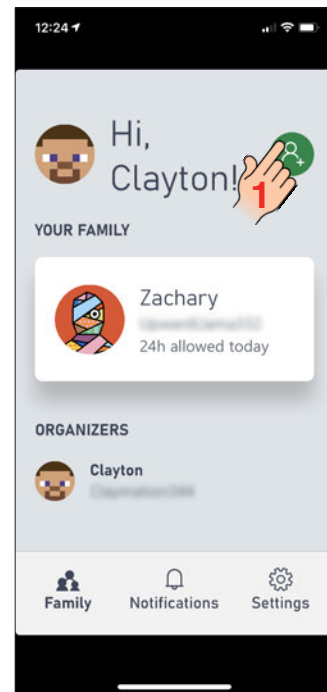
Sign in to the app with an organizer's (parent's) Microsoft account, and then select **Continue**.

1. Select the green Accounts icon in the top right of the Family screen, select **Invite someone**, and then select **Next**.
 2. Enter the **email address** of the member you want to add, and then select **Next**.
- Verify that Member is selected for their role in the family group, and then select **Send Invitation > Done**. We'll email an invitation to the member's email address.

Note: You'll need to open the email invitation that was sent to the member's email, select **My parent can sign in now**, and follow the on-screen instructions.

Sign out and then back in to the app with an organizer's Microsoft account, and then make sure the member's account was added Your family.

If the member's account doesn't have an Xbox profile, select **Set up Xbox account** under their account name and follow the on-screen instructions to create one.



Add a child that does not have a Microsoft account

Sign in to the app with an organizer's Microsoft account, and then select **Continue**.

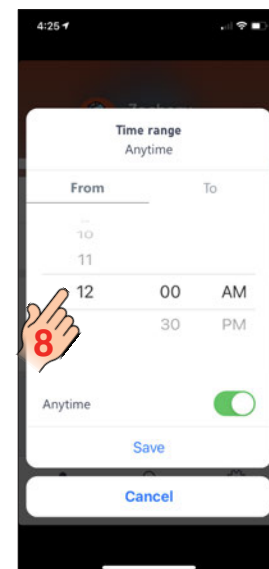
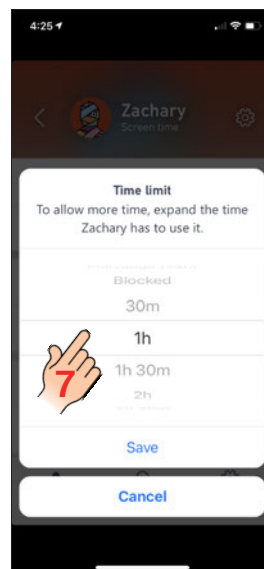
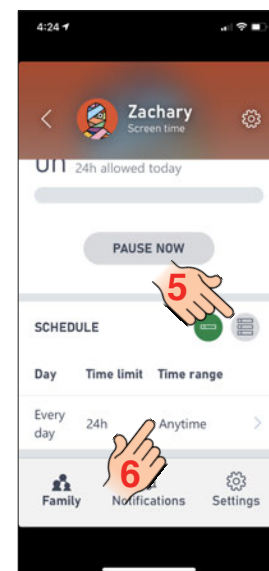
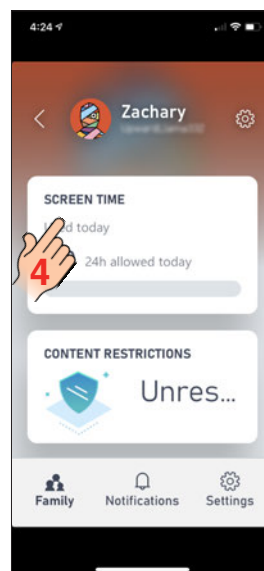
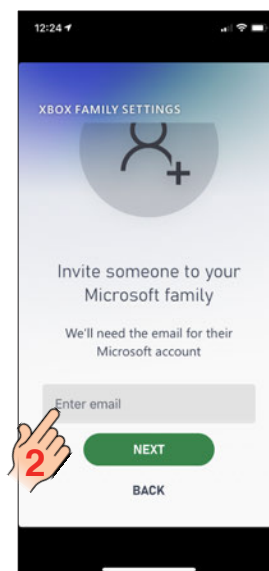
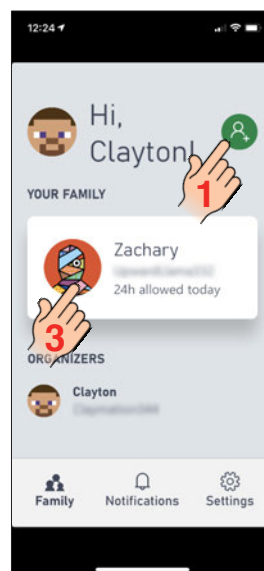
1. Select the green **Accounts icon** in the top right of the Family screen, select **Create a child account**, and then select **Next**.
2. Enter the member's **email address**, or select **Get a new email address** to get a new one.

Follow the on-screen instructions to set up the member's Microsoft account.

After the app automatically generates a gamerpic and gamertag for the member's Xbox profile, select Next.

Manage Screen Time

3. Tap on your **child's profile card**.
4. Tap on the **Screen Time card**.
5. Choose the **Schedule** you prefer, the same time limit for every day of the week or customize the time limits daily.
6. Tap on the day you want to limit screen time on.
7. Choose the **Time limit**, the total allowed screen time for that day.
8. Choose the **Time range** that your child can use the Xbox.

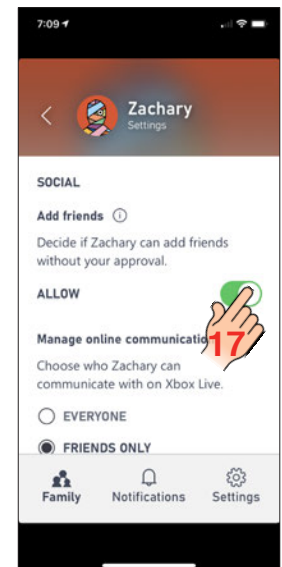
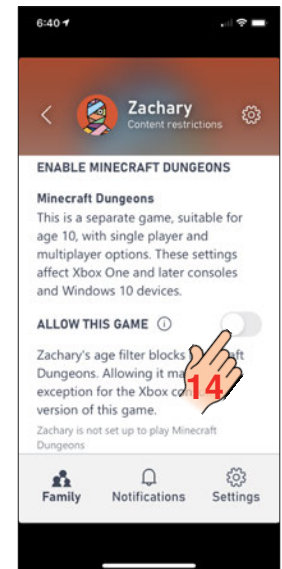
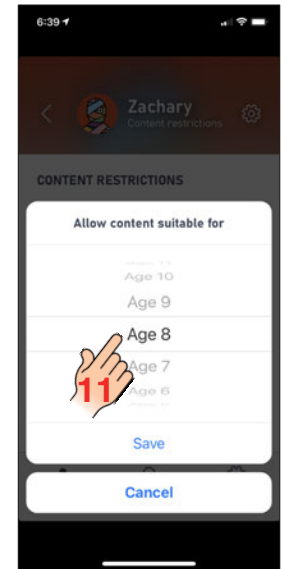
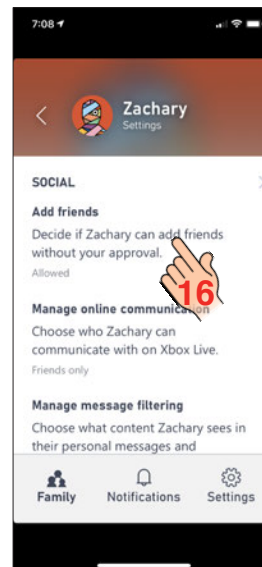
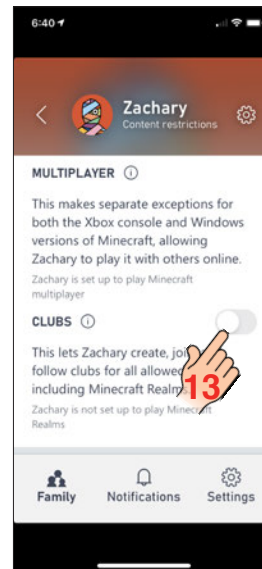
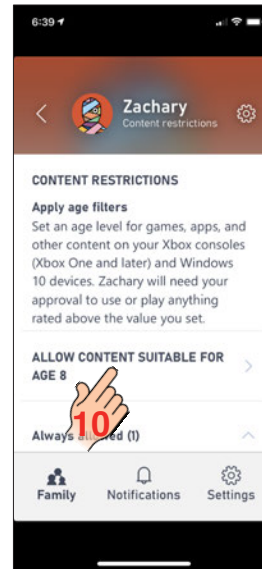
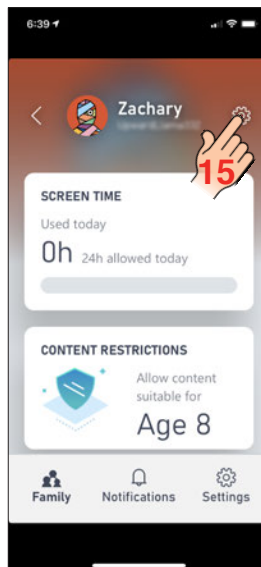
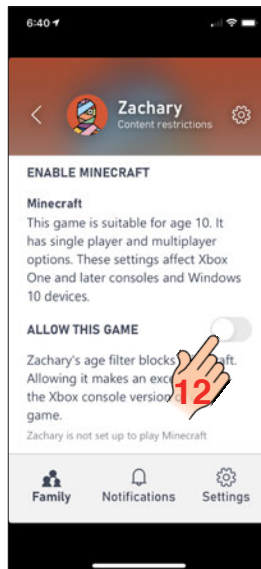
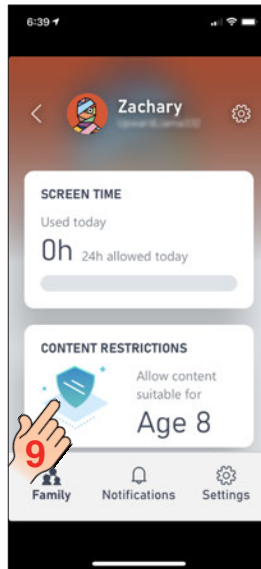


Apply age filter for your child's Xbox games

- Tap on your **child's profile card**.
9. Tap on **Content Restrictions**.
 10. Tap on **Allow Content** to set the appropriate content age level for your child.
 - If you set your child's age below 10-years-old, you will have to toggle on Minecraft.
 12. Toggle on **Allow this game** to enable Minecraft.
 13. Clubs are online meeting places created by the Xbox community for like-minded people to enjoy multiplayer gaming and socializing. **I do not recommend enabling this for children under the age of 16-years-old.**
 14. Toggle on **Allow this game** to enable Minecraft Dungeons.

Control friend approval

15. Tap on the **gear icon** in the top right corner of the app.
16. Select **Add friends**.
17. If you want to approve every friend request, leave this toggled off (greyed out). If you toggle it on, choose **Friends Only** below.



Manage online communication

1. This is who your child can communicate with using voice and text, and who can send them invitations to parties, games, or clubs. Select the appropriate one:
- **Everyone** means anyone signed into the Xbox online community.
 - **Friends** are anyone in your child's Xbox live friends list.
 - **No one** means your child will not receive any voice or text communications or invites.

Manage message filtering

2. You can choose the default filtering for your child's age. If you choose **Custom**, you can set the filter level granularly for a variety of texting situations.
3. Be sure **View hidden content** is turned off (greyed out)

Manage online purchases

4. Toggle Ask to buy **ON** (green)

Manage multiplayer gaming

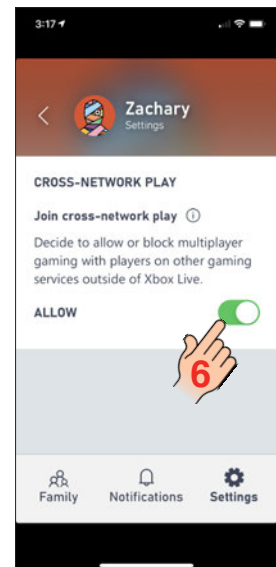
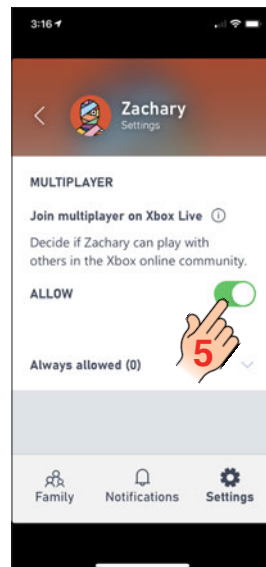
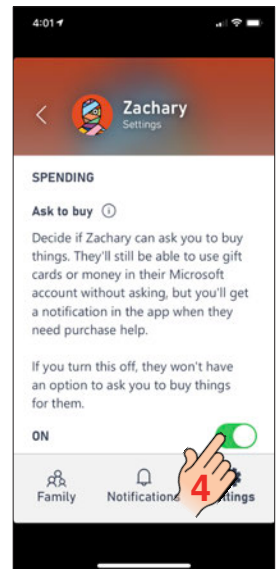
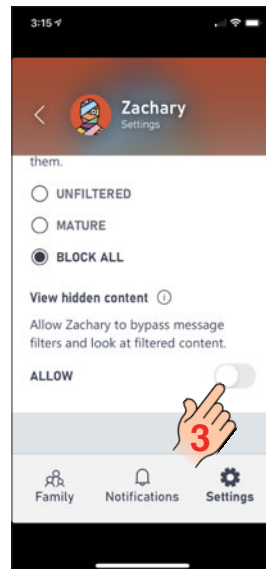
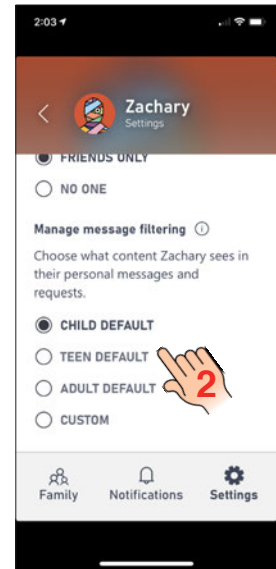
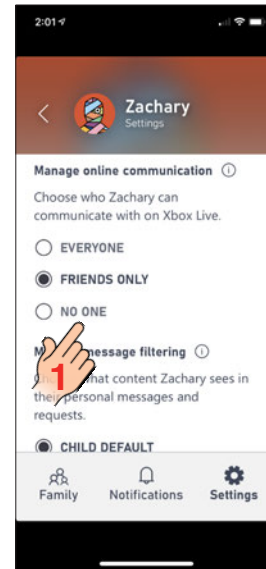
5. Toggle off if you do not want your child playing multiplayer games

Manage cross-networked games

Some multiplayer games can be played by people on different platforms, such as PC and Nintendo.

6. Toggling this off will block your child from playing these games.

Note: There is nothing inherently more dangerous about cross-networked games as opposed to multiplayer. They are essentially the same thing.



Block inappropriate websites on your Xbox

Web filtering is on automatically on for kids under 8.)

Method One: On the console

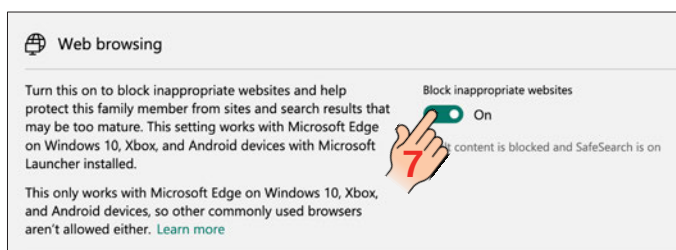
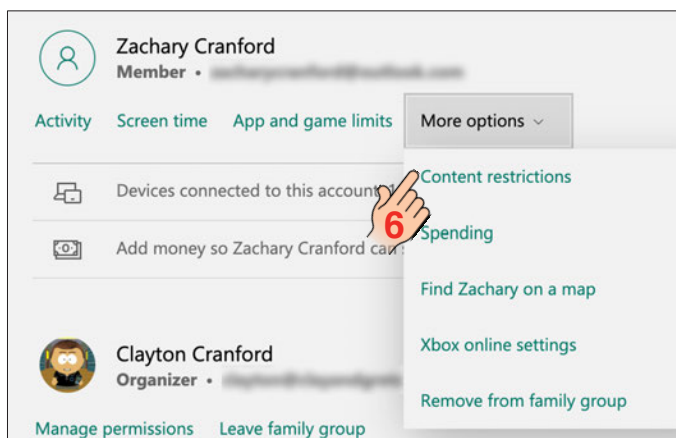
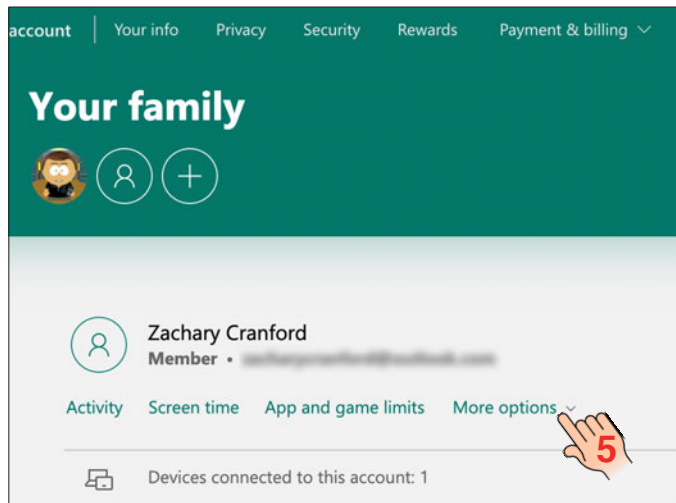
1. On the console's controller, press the Xbox button to open the guide, and then go to **Profile & system > Settings > Account > Family settings**.
2. Select **Manage family members**, and then choose the child account to which you want to add web filters.
3. Select **Web filtering**, and then select the drop-down menu to view all the available options.
4. Choose the desired level of web filtering.

Note: If you choose Allow list only, your child can only view the websites you've added to the Always allowed list on account.microsoft.com/family.

Method Two: On your Microsoft account

Log into your account at:
account.microsoft.com/family.

5. Click on More options under your child's account.
6. Click Content restrictions
7. Toggle on Web browsing.
8. You can list website you do not want blocked and website you want blocked (e.g., reddit.com, omegle.com, etc.).
9. Check Only allow these websites to restrict your child to specific sites you choose





PlayStation 4 & 5 Parental Controls

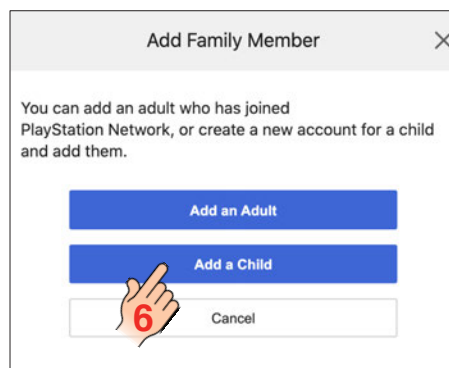
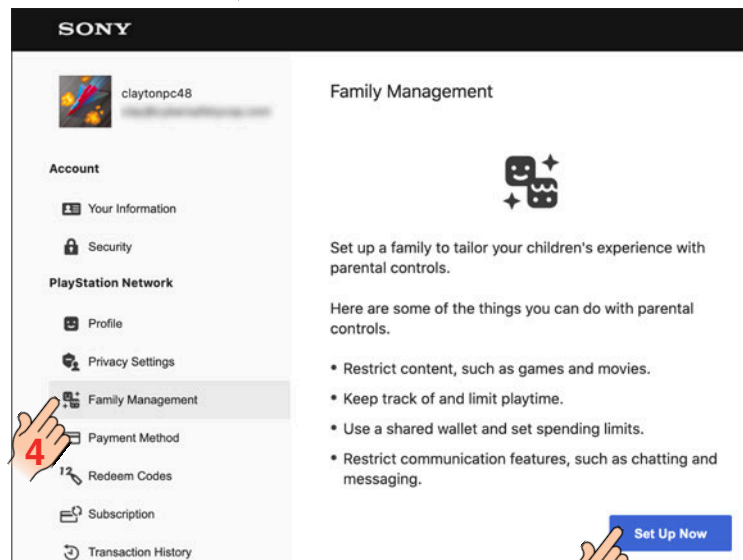
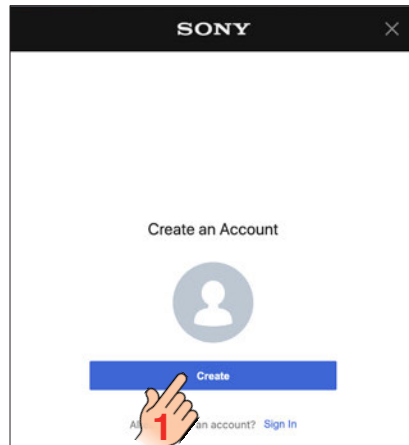
Set up an the parent's account for PlayStation Network

You need an account to use PlayStation Network services. It's free to create an account and you do not need to provide any payment details.

1. From your web browser, go to Account Management (<https://id.sonyentertainmentnetwork.com/>) and select **Create New Account**.
2. Enter your details and preferences and select **Next** on each screen.
3. Verify your email address. Check your email for a verification message. Follow the instructions in the message to verify your email address.

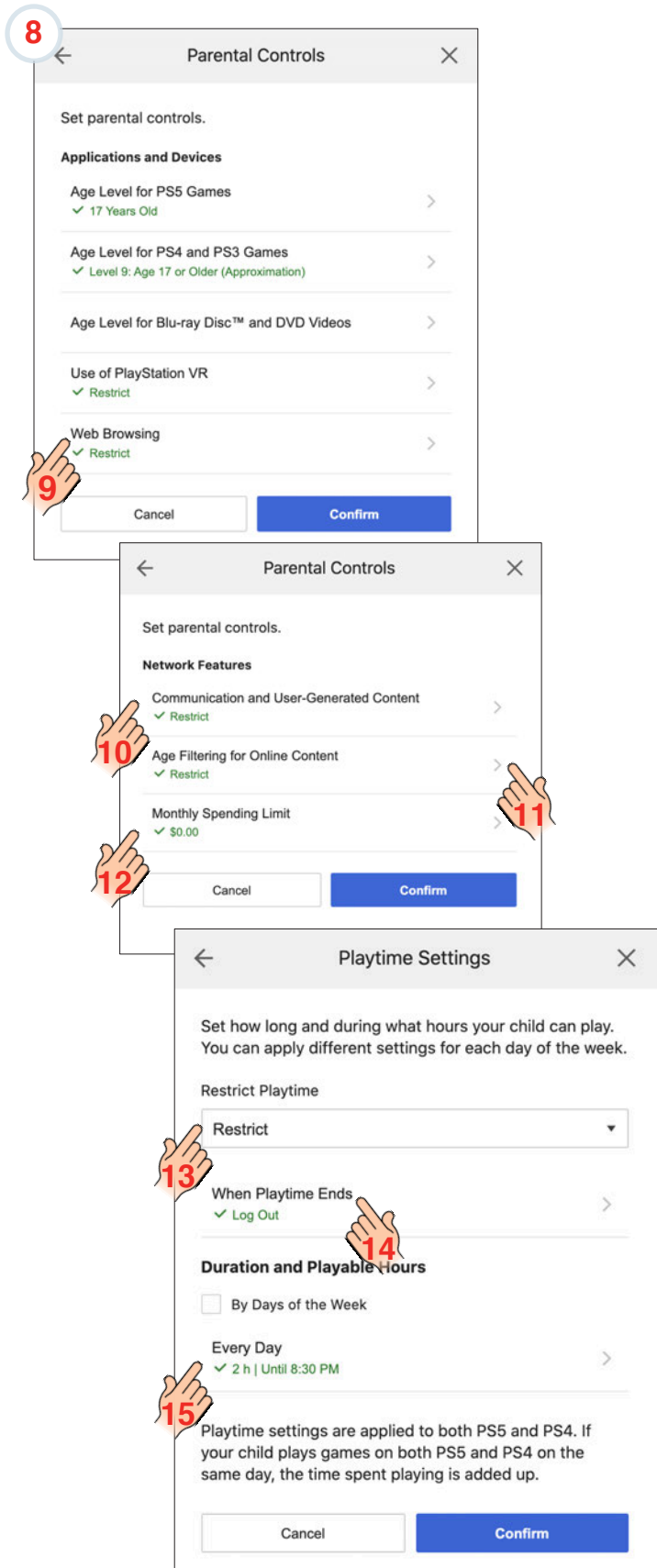
Adding a child's account

4. Sign in to Account Management, and select Family Management.
5. If you have not set up a secondary account yet, select **Set Up Now**. Otherwise, select **Add Family Member**.
6. Select **Add a Child**.
7. Enter the child's name and date of birth, then click **Next**. The User Agreement will appear and you'll need to accept this to continue.



8. Select the appropriate age for your child.
9. Choosing restricted **Web Browsing** will restrict using the web browser to open URLs shared in messages and links to web pages within games. Set Restrict for children under the age of 16. If you are concerned about your child getting links to pornography, restrict. Then select **Confirm**.
10. For younger players, I recommend restrict chatting and messaging with other players (including your child's friends), as well as viewing or sharing videos, images, and text on PlayStation Network.
11. Restrict access to online features of PS4 games, and hide games and content in PlayStation Store based on your child's age.
12. Limit the total amount your child can spend in PlayStation Store in a calendar month. Payments are made from the family manager's wallet. Then select **Confirm** and set your timezone.
13. Restrict **Playtime**.
14. Set **Log out** when playtime ends.
15. Set how long and during what hours your child can play. You can apply different settings for each day of the week.

Note: Playtime settings are applied to both PS5 and PS4. If your child plays games on both PS5 and PS4 on the same day, the time spent playing is added up.



Prevent children from changing parental controls on PlayStation 5 and PlayStation 4

There are three more important steps to secure and protect your child on their PlayStation.

Set a system restriction passcode

The system restriction passcode prevents your child from changing parental controls settings on your PlayStation. Make sure to choose a memorable passcode that only you know. Only share it with the family member(s) you appoint as guardian because it enables all controls to be changed or removed.

1. Sign in as the family manager and go **Settings > Family and Parental Controls > PS5 Console Restrictions**, or **PS4 System Restrictions**, depending on the console.
2. Enter the existing system restriction passcode. If you haven't set one before, the default is 0000.
3. Select **Change Your System Restriction Passcode**.
4. Enter a new four-digit passcode using the corresponding buttons on the controller. Make sure it's something memorable that only you know.
5. Enter the passcode a second time to confirm.

Set a login passcode

Make everyone who has an account on your PlayStation console to set a login passcode. Otherwise, your child family members can log in to the accounts of adults or older children and avoid the controls you have placed on them.

For a PS5

1. Go to **Settings > Users and Accounts**.
2. Select **Login Settings > Set a PS5 Login Passcode**.
3. Set a four-digit passcode. Make sure it's something memorable that only you know.

For a PS4

1. Go to **Settings > Login Settings > Login Passcode Management**.
2. Set a four-digit passcode. Make sure it's something memorable that only you know.

Disable new user creation and guest login

Prevent your child from creating a new unrestricted account instead of using the one you created for them by disabling new user creation and the option to log in as a guest.

1. Log in as the family manager and go to **Settings > Family and Parental Controls > PS5 Console Restrictions** or **PS4 System Restrictions**.
2. Select **User Creation and Guest Login > Not Allowed**.



Nintendo Switch Parental Controls

To set up parental controls on your child's Nintendo Switch, you must create an account at <https://www.nintendo.com/>

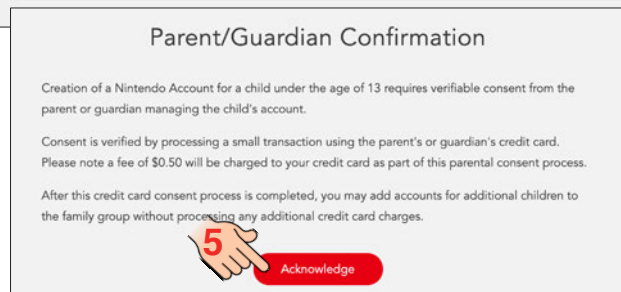
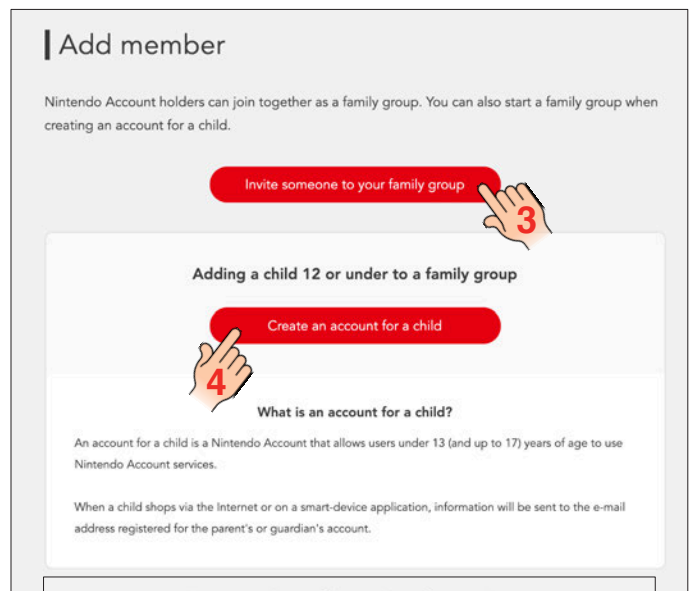
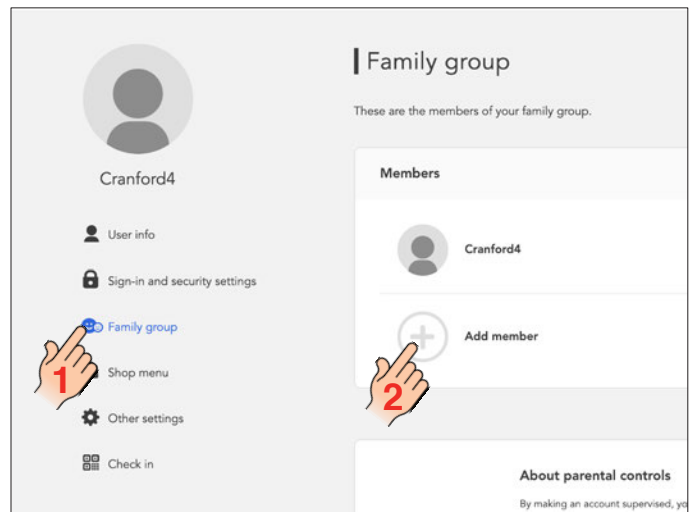
1. Sign into your Nintendo account and select **Family Group**.
2. Select **Add member**.

If your child already has their own Nintendo account

3. Select **Invite someone to your family group**.

If your child does not already have an account.

4. Select **Create an account for a child**.
5. You will need your credit card to prove you are a parent setting up their child's account. It will only cost \$.50.
6. Follow the directions on the proceeding screens.



7. From the Family group settings page, select your child under the Members.
8. Select **Spending/purchases on Nintendo Switch eShop and nintendo.com**.
9. If you want to restrict your child from purchasing games or subscriptions, then check **Restricted** and **Save changes**.
10. Select **Viewing of content on Nintendo Switch eShop**.
11. Check the box to restrict your child to only view content based on their age and ESRB rating categories.



Nintendo parental controls and screen time use are set up and controlled by

Nintendo's free app, Nintendo Switch Parental Controls. Download it from either the Apple App Store or Google Play.

12. Have your child's Switch nearby. Open the app and tap, **Next**.
13. Now, you will link the app to your child's Switch. Follow the Instructions provided.
14. Once the Switch is linked, you can now configure the parental controls. From the settings screen, select **Play Time Limit** card.

Settings for family group members

zachary Supervised

Date of birth 4/4/2013

Gender Male

Country/region of residence United States

Parental controls A parent or guardian in your family group has applied the following to your account:

- Spending/purchases on Nintendo Switch eShop and nintendo.com
- Viewing of content on Nintendo Switch eShop
- Restrictions on sharing of your account information with third party services (parent/guardian confirmation required each time)

User info >

Sign-in and security settings >

Spending/purchases on Nintendo Switch eShop and nintendo.com >

Viewing of content on Nintendo Switch eShop >

Other settings >

Settings for family group members

zachary Supervised

Spending/purchases on Nintendo Switch eShop and nintendo.com

Nintendo Account parental controls do not apply to purchases made on U systems, so please use one of those devices to add those restrictions.

To restrict this user's spending/purchases (including automatic renewal of subscriptions) on Nintendo Switch eShop and nintendo.com, check the box and then select "Save changes."

☒ Restricted

Save changes

Settings for family group members

zachary Supervised

Viewing of content on Nintendo Switch eShop

If restricted, the Nintendo Switch eShop content this user can see will depend on their age and the relevant ESRB rating categories.

To restrict this user's viewing of content on Nintendo Switch eShop, check the box and then select "Save changes."

☒ Restricted

Save changes

App Linking Screens:

3:58 App Store

A Nintendo Switch console will be linked to this app.

Please ready your Nintendo Switch console.

Next

13

Enter the code below on the Nintendo Switch console.

The Nintendo Switch console will be linked to this app. Please follow the instructions listed below.

Registration code: 481513

Instructions

1 Switch the Nintendo Switch console on.

6:10 Switch #1

Disable Alerts for Today

Play Time Limit Until 20:30

Whitelist

Restriction Level Child

PIN

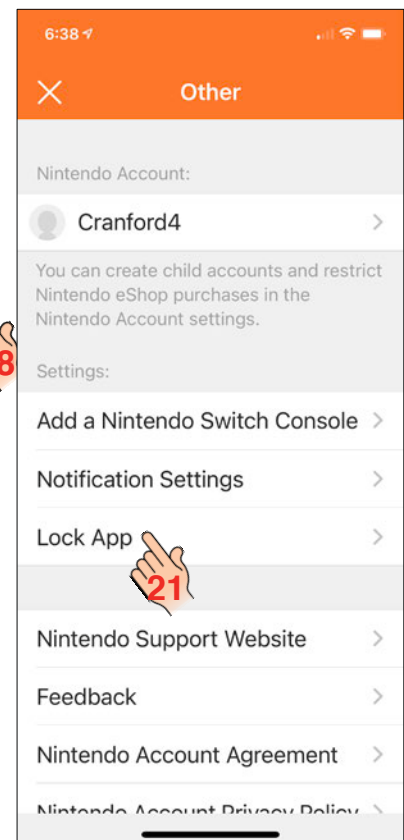
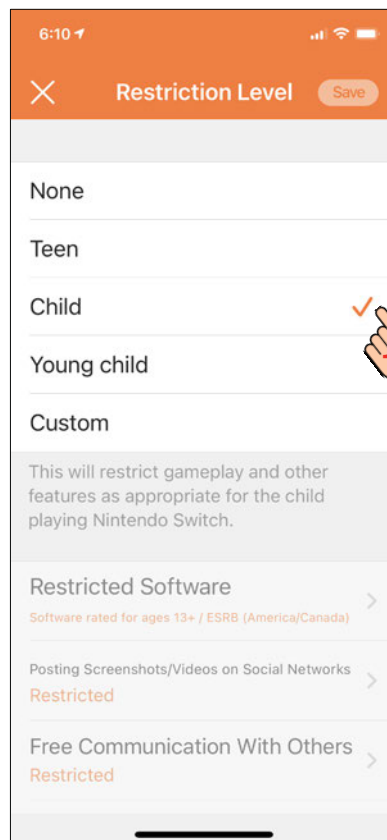
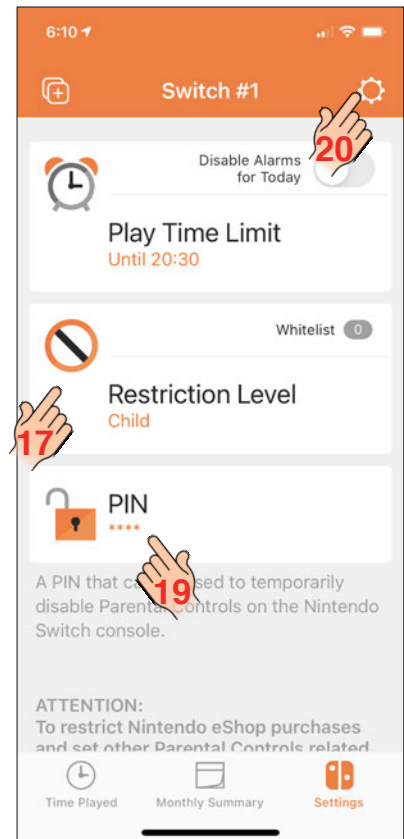
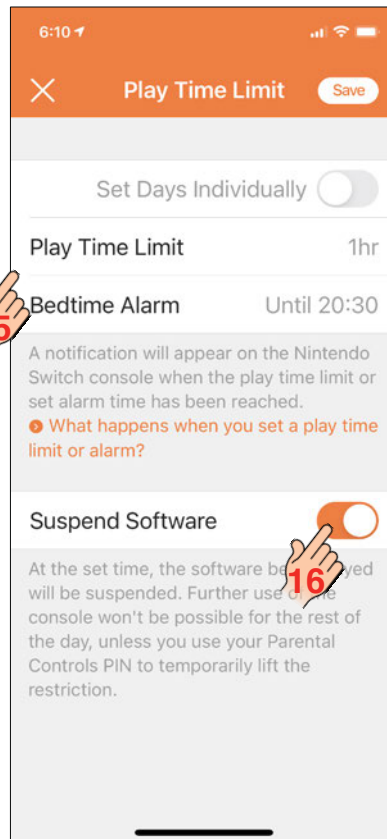
A PIN that can be used to temporarily disable Parental Controls on the Nintendo Switch console.

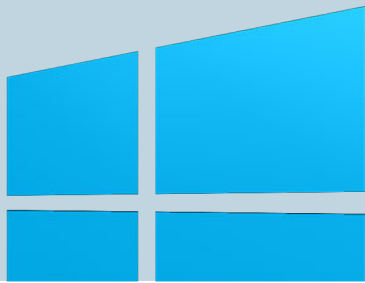
ATTENTION: To restrict Nintendo eShop purchases and set other Parental Controls related

Time Played Monthly Summary Settings

If you have set both a daily play time limit and a bedtime alarm, a notification will appear on your child's Nintendo Switch for whichever limit is reached first. You can temporarily disable Parental Controls in order to allow unrestricted play on the device. Your Parental Control PIN is required to disable Parental Controls.

15. Set the maximum play time and when bedtime begins and ends.
16. Toggle **Suspend Software** on and then select **Save**.
17. Select the **Restriction Level** card on the settings screen.
18. You can choose from three pre-configured levels (Teen, Child, and Young Child), or you can Customize your child's restriction level. Then select **Save**.
19. Select the PIN card on the settings screen. Set a unique PIN.
20. To secure your parental control settings from being changed, select the cog icon on the settings screen.
21. Select **Lock App** and enable either Touch ID or Face ID (whichever your device has).





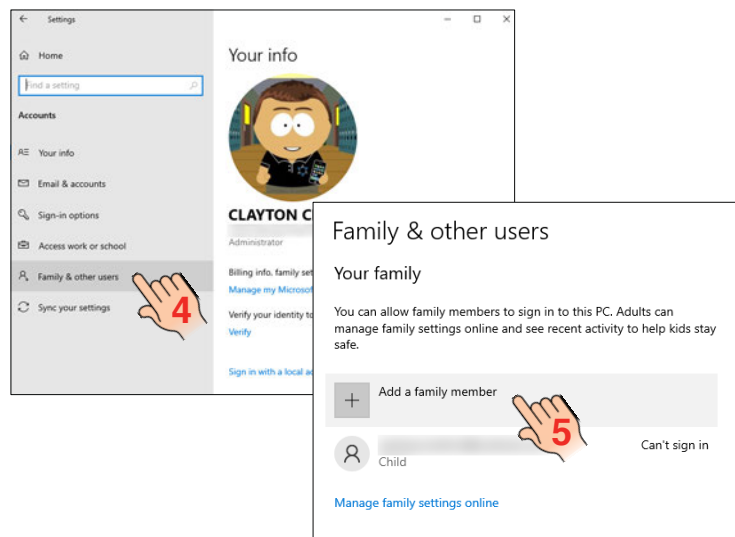
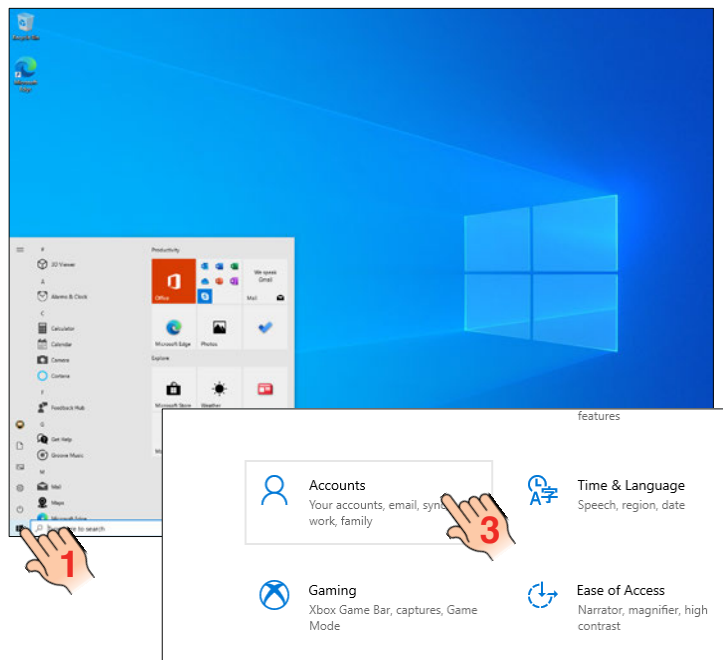


Windows 10 Parental Controls

Microsoft gives you a couple of ways to set up parental controls on your child's Windows 10 device. First, you must create a Microsoft account and set up a Family account. This can be done on your Windows 10 device or online. Additionally, Microsoft also has a mobile app, Microsoft Family Safety (iPhone and Android), that can control screen time, content filters, family location tracker, and driving reports.

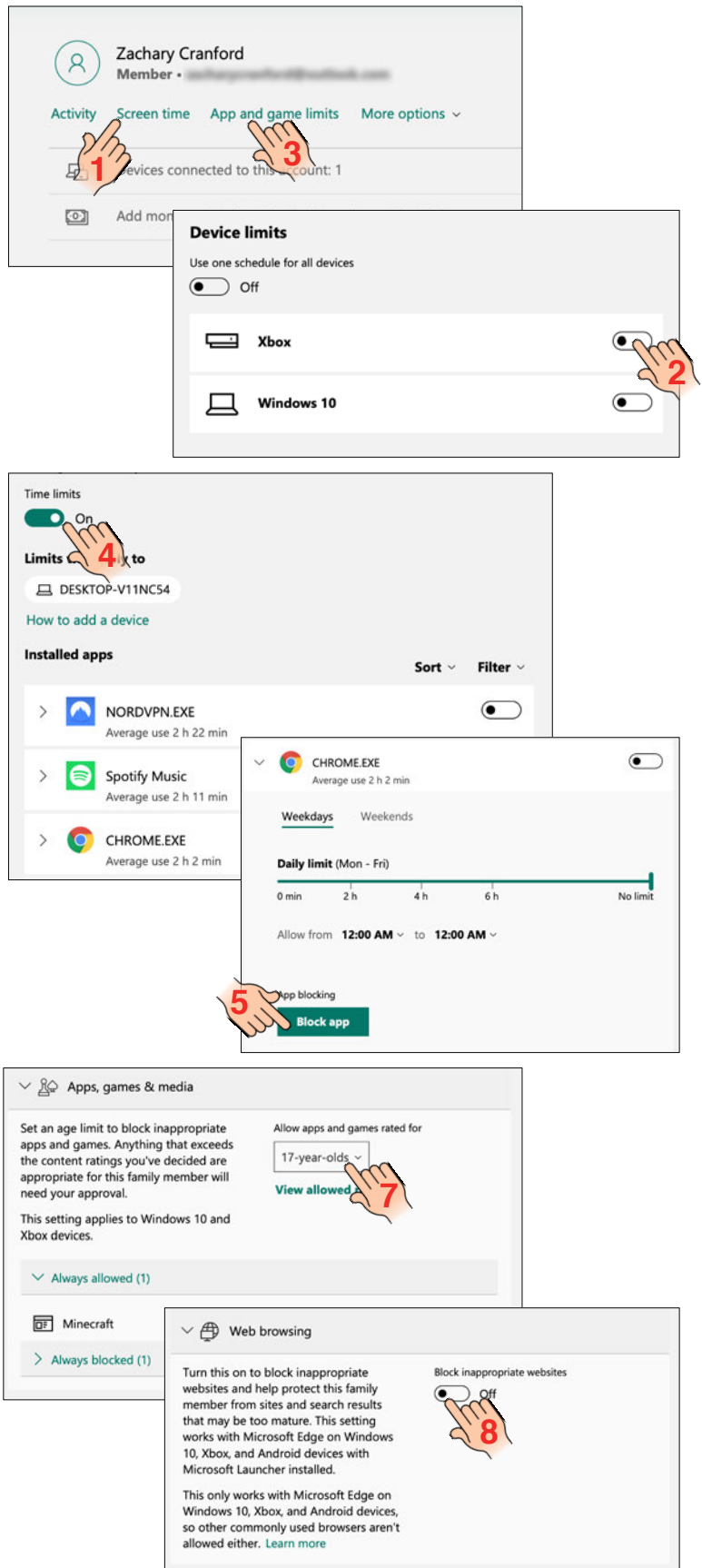
Create add a child to a Microsoft Family from a Windows 10 computer.

1. Log onto your Windows computer and select the  icon.
2. Select the Settings  icon.
3. Select **Accounts**.
4. Select **Family & other users**.
5. Select **Add a family member**.
6. If your child already has a Microsoft account, enter the associated email. If they do not have a Microsoft account, select **Create one for a child**.
7. Create their new outlook email and follow the steps to set up their account. This will be the information they will use to log into their Windows computer.
8. Finally, open up your child's email account. If you're setting up their Microsoft account for the first time, you'll find two confirmation requests from Microsoft waiting for their attention – one to verify their email address and one accept parental supervision of their account.



To make changes to your child's parental controls, from your Internet browser, log into www.account.microsoft.com/family. You can also make these changes on the Microsoft Family Safety App.

1. From the Family screen, select **Screen Time** under your child's account.
2. Toggle on the linked devices that you want to put screen time limits on.
3. Select **App and game limits**.
4. Toggle on **Time Limits**.
5. To block your child from using an app, select **Block app**.
6. Select **Content restrictions**.
7. Choose the appropriate age rating for your child's available games. You will also see a list of the Apps you have designated as **Always allowed** and **Always blocked**.
8. Toggle on **Block inappropriate websites** under **Web browsing**. This setting only works with Microsoft Edge Internet browser on Windows 10, Xbox, and Android devices with Microsoft launcher installed. Consequently, it will automatically block the most commonly used browsers. If your child needs Chrome Browser for school work, you will need to unblock it. It will not be covered by this parental control.



9. Select **Spending**.

10. Toggle on **Needs organizer approval to buy things** and **Email me when they get stuff**.

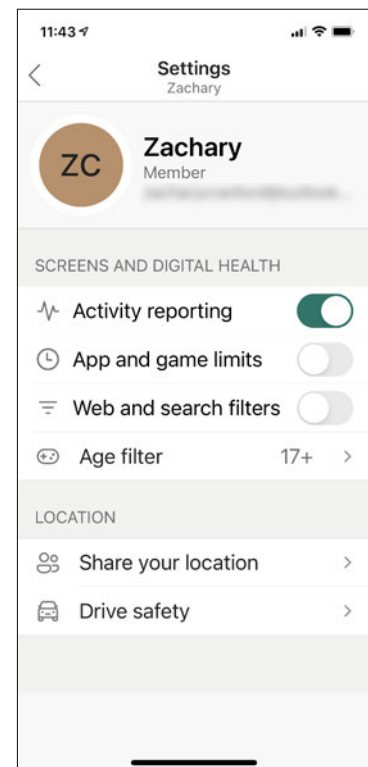
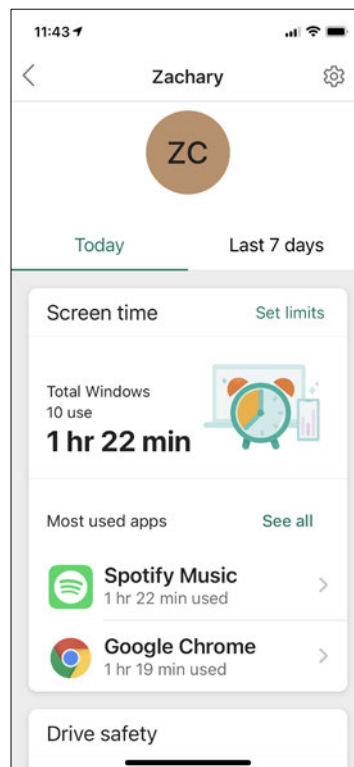
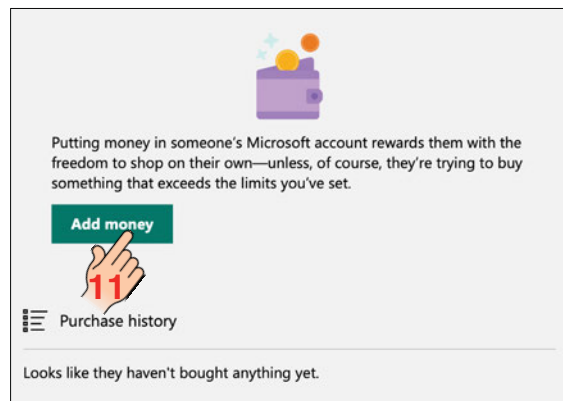
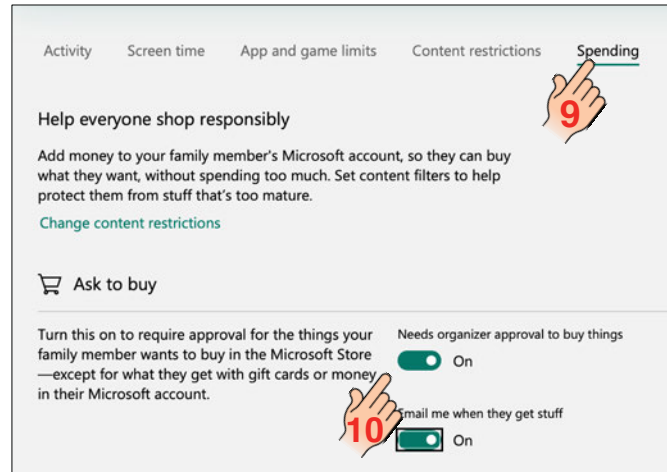
11. If you want to fund your child's account with money that they can use on games, select **Add money**. You can also see their purchase history here.



Microsoft Family Safety app
Install the Microsoft Family Safety app on your mobile device.

It will allow you to easily see your child's screen time activity across all of their linked Microsoft devices (Xbox included).

You can adjust any of the parental controls mentioned above. Additionally, if you are a Microsoft 365 Family subscription, you can get location alerts when someone leaves or arrives at a designated location. Get insights on how your family is doing on the road, including how many times they use their phone while driving, their top speed, and even the number of times they brake hard.



macOS Parental Controls




To set up parental controls on your macOS devices, you must first set up Family Sharing. If you have already done this, skip ahead to “Set up Parental Controls.” The screen shots are from macOS Big Sur 11.0.

Set up Family Sharing on Mac

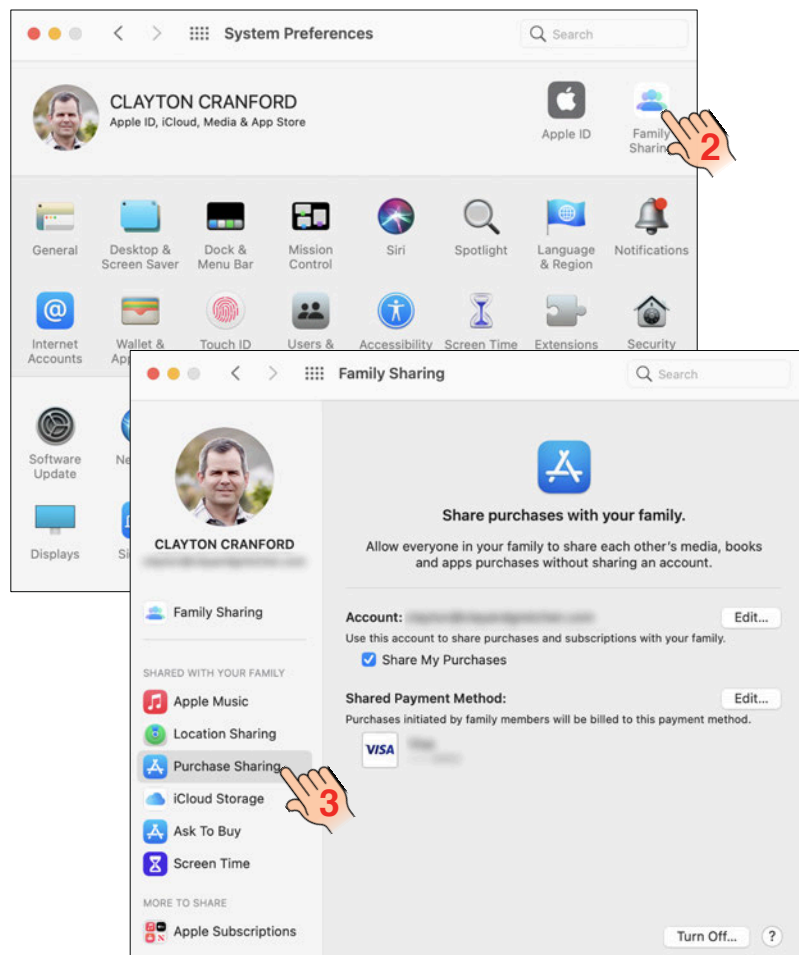
Family Sharing lets up to six members of your family share iTunes Store, App Store, and Apple Books purchases, and an iCloud storage plan—all without sharing accounts. Your family can share subscriptions to Apple Music, Apple TV, Apple News+, and Apple Arcade (not available in all countries or regions). Your family can also help locate each other’s devices with the Find My app on the Mac, on iCloud.com, and on iOS and iPadOS devices. One adult, the family organizer, sets up Family Sharing and invites up to five people to join the Family Sharing group.

On your Mac

1. Select the **Settings**  icon in your Applications folder.
2. Select **Family Sharing**.
3. Confirm the Apple ID that you want to use for Family Sharing, and make sure that Share My Purchases is selected.


4. Follow the onscreen instructions.
If you're using macOS Mojave or earlier:

1. Select the Settings icon in your Applications folder, then click iCloud.
2. Confirm the Apple ID that you want to use for Family Sharing, and make sure that Share My Purchases is selected.
3. Follow the onscreen instructions.



Set up Parental Controls

On your Mac, do one of the following:

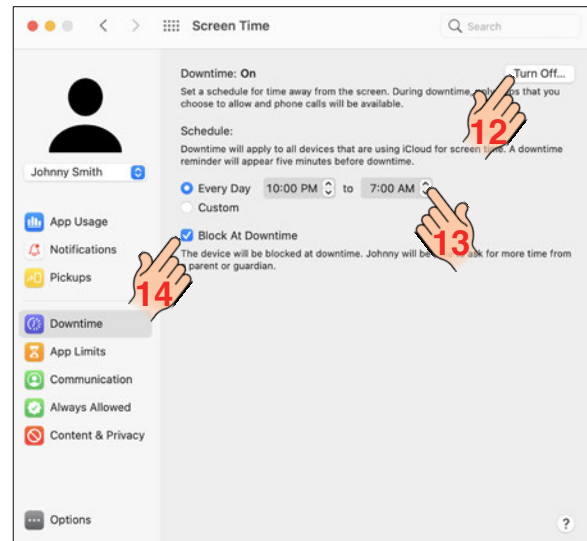
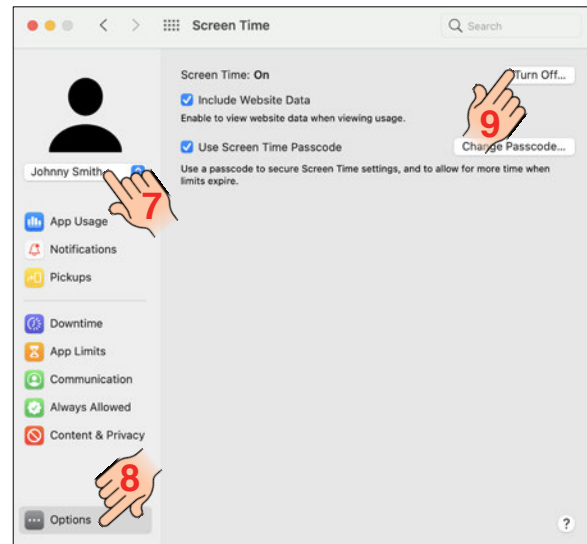
4. If you're using Family Sharing: Log in to your Mac user account, then make sure you're signed in with your Apple ID.
5. If you aren't using Family Sharing: Log in to the child's Mac user account.
6. From the System Preferences window, click Screen Time .
7. If you're using Family Sharing, click the pop-up menu in the sidebar, then choose a child.
8. Click **Options** in the lower-left corner of the sidebar.
9. Click **Turn On** in the upper-right corner.

Select any of the following options:

10. Include Website Data: Select this option if you want Screen Time reports to include details about the specific websites visited. If you don't select this option, websites are just reported as Safari usage.
11. Use Screen Time Passcode: Select this option to keep Screen Time settings from being changed, and to require a passcode to allow additional time when limits expire.

Set up Downtime

12. If Downtime is off, click Turn On in the upper-right corner. If the Turn On button is dimmed, you need to turn on Screen Time for the selected family member.
13. Choose your Downtime schedule.
14. If you want to block the device during downtime, select the Block At Downtime checkbox. This option is available only when you're using a Screen Time passcode.



Set up app limits

In Screen Time on Mac, you can set time limits for apps and websites for yourself or your children.

15. Click **App Limits** in the sidebar.

16. If App Limits is off, click **Turn On** in the upper-right corner. If the Turn On button is dimmed, you need to turn on Screen Time.

17. Click the **+** button to create a new app limit.

You can include any combination of apps, categories, or websites in each limit you create.

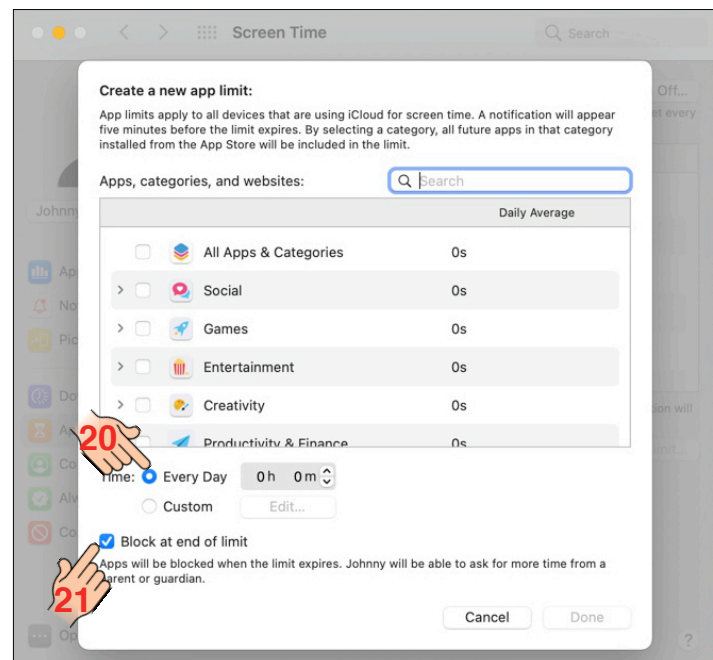
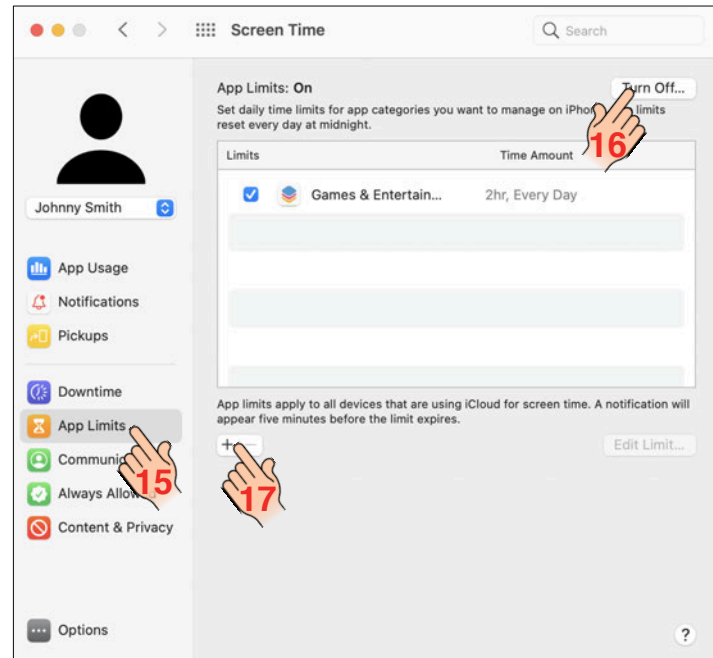
18. In the “Create a new app limit” window, select the checkbox next to each of the apps, categories, or websites that you want to include in the limit.

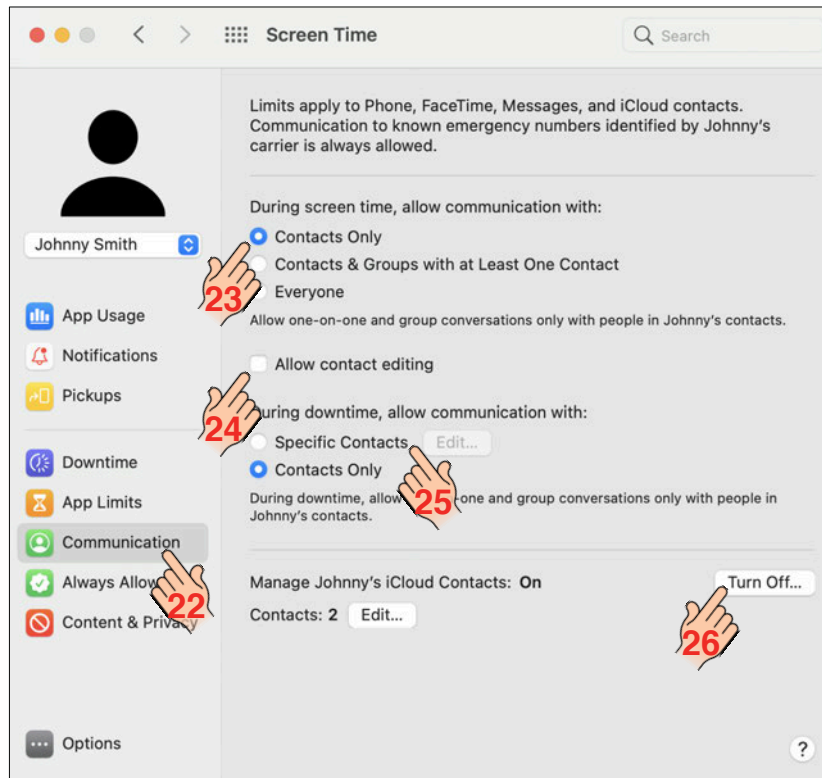
19. Limit a website: Click the arrow next to the category Websites at the bottom of the list. If the website has been visited, it appears in the list below the Website category, and you can select the checkbox next to it. If the website isn’t in the list, click the Add Website button below the website list, then type the URL for the website.

Enter a limit in the Time field:

20. Set up the same app limit for every day: Select **Every Day**, then enter an amount of time. Set up a different app limit for each day of the week: Select **Custom**, then enter an amount of time for each day.

21. Click **Block at end of limit** and **Done**.





Set up communication limits

The limits you set apply to phone calls, FaceTime, Messages, and iCloud contacts. A parent or guardian can also request permission to manage a child's iCloud contacts.

22. Click **Communication** in the sidebar.

23. Select an option below “During screen time, allow communication with.”

- **Contacts Only:** Allow one-on-one and group conversations during screen time only with people in your family member's contacts.
- **Contacts & Groups with at Least One Contact:** Allow one-on-one conversations during screen time only with people in your family member's contacts, and allow group conversations that include at least one person in your family member's contacts.
- **Everyone:** Allow one-on-one and group conversations during screen time with anyone, including unknown numbers.

24. Leave this option unselected if you want to prevent your child from editing their contacts.

25. Select **Specific Contacts** under “During downtime, allow communication with.”

26. If you want to manage a child's iCloud contacts, click the **Turn On** button.

If your family member denies the request to manage their contacts, the Pending status is no longer displayed.

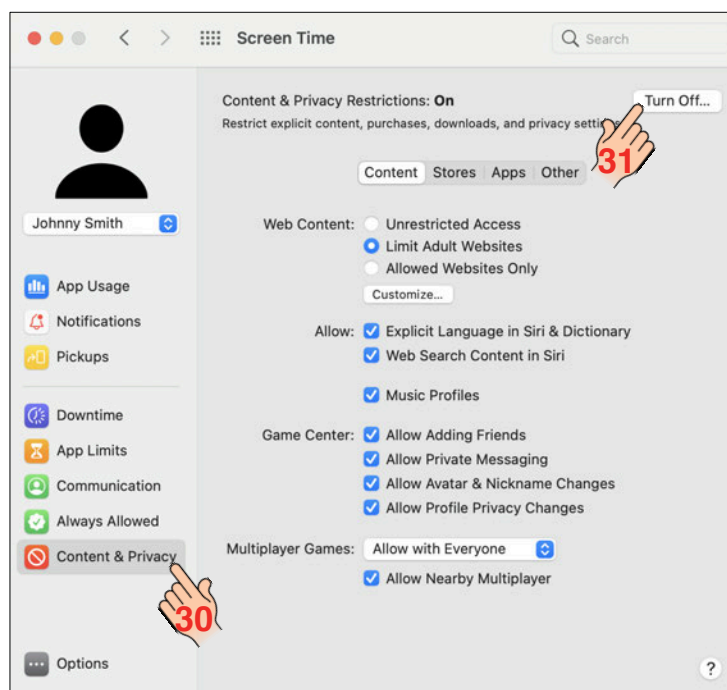
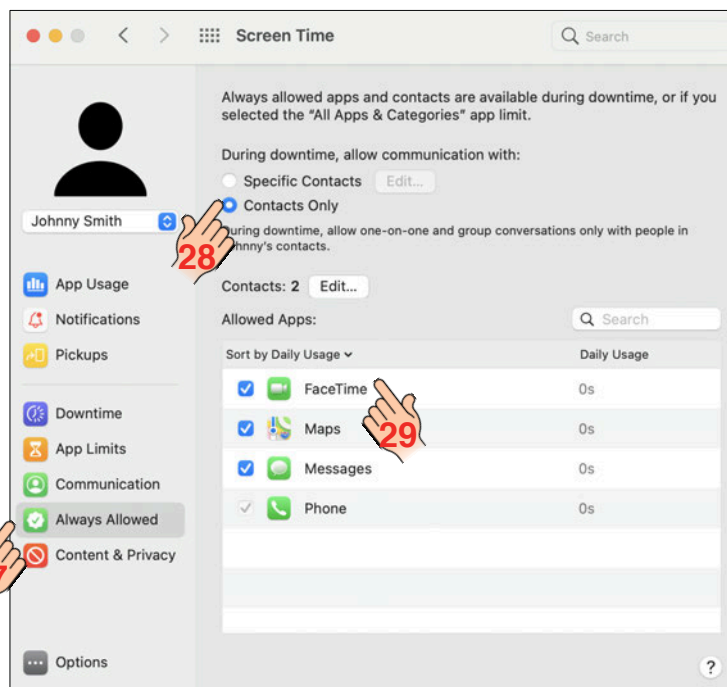
Choose always allowed apps in Screen Time

Specify apps that can be used anytime, even during downtime, for your child.

27. Click **Always Allowed** in the sidebar.
28. Select an option below “During downtime, allow communication with.” See “Set up communication limits.”
29. In the list of Allowed Apps, select or deselect the checkboxes next to the apps.

Set up content and privacy restrictions

30. Click **Content & Privacy** in the sidebar.
31. If Content & Privacy Restrictions are off, click **Turn On**.
32. To restrict web content, click **Content**, then select options.
 - Select **Limit Adult Websites** or **Allowed Websites Only**
33. To restrict movies, TV shows, and app purchases, click **Stores**, then select options.
 - Check **Always Require Password**
34. To restrict apps, click **Apps**, then select options.
 - Uncheck **AirDrop**
35. To lock certain settings, click **Other**, then select options.
 - Make sure **Account Changes** is unchecked.






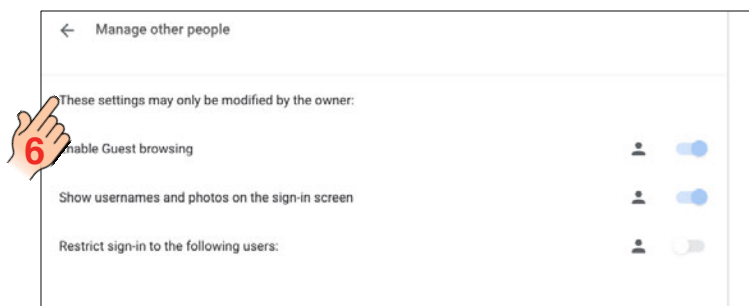
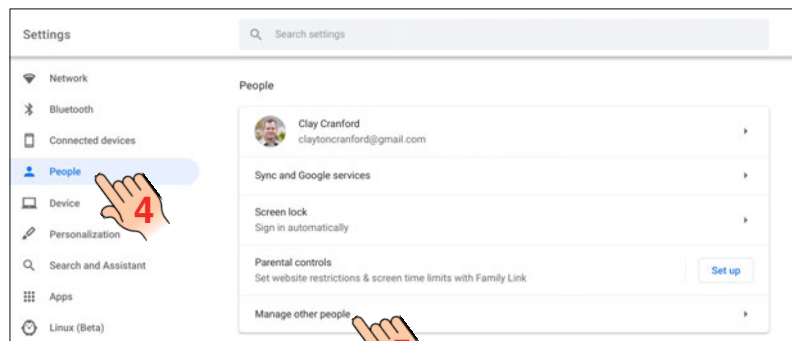
Chromebook Parental Controls

Chromebooks are a new type of computer that run on Chrome OS, an operating system that has cloud storage, Google built-in, and multiple layers of security. Many schools are providing Chromebooks to their students to use in the classroom or to take home. Depending on your situation, you may be providing the Chromebook for your child, or the school may own the Chromebook your child is using at home. Like all computers, parental controls need to be used. A school owned Chromebook may pose some challenges. We will provide solutions for both situations.

Situation 1: School owned Chromebook

Your child's school Chromebook account will have controls to block inappropriate websites. If the Chromebook is configured to allow "guest" logins, anyone can login with a non-school Google account and bypass all the school controls. Also, we want the Chromebook to be restricted to only allow certain accounts access to it. The first step is to determine if your child's school Chromebook allows "guest browsing."

1. Turn on your child's Chromebook. On the login screen, if the option "Browse as Guest" appears on the bottom left area of the screen, then Guest Browsing is turned on.
2. Log into your child's account, click on the clock area in the bottom right corner of your screen.
3. Click on the cog  icon (Settings).
4. Select **People**.
5. Select **Manage other people**.
6. If you see **These settings may only be modified by the owner**, you will not be able to turn off guest browsing and turn on Restrict sign-in. You will need to contact the school's IT administrator and have them make these changes.

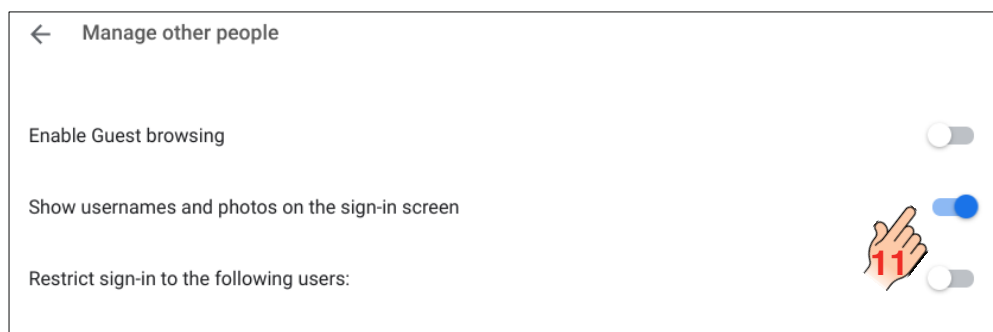



Situation 2: Parent owned Chromebook

A parent owned Chromebook is by far the best situation to be in. It will give the parent the flexibility to set up their child's account and use Family Link to unify parental control settings across all of their Google/Android devices.

Make a parent the Owner of the Chromebook.

The first step is to make a parent the “owner” of the Chromebook. If your child has already created an account on their Chromebook, perform a factory reset. They will not lose their files as they are saved in the cloud. To perform a factory reset: Sign out of your Chromebook, and press and hold Ctrl + Alt + Shift + r.



7. Sign in as the owner. You will need a Google account to do this.
8. In the bottom right corner of your screen, click on the clock area .
9. Click the gear icon  (Settings).
10. Select **People**, then select **Manage other people**.
11. Ensure **Enable Guest browsing** is toggled off (white), **Show usernames and photos on the sign-in screen** is toggled on (blue), and **Restrict sign-in to the following users** is toggled off (white). We will be coming back to toggle this on after we have added your child's account.


Add your child to the Chromebook

12. If you're signed in to your Chromebook, sign out.
13. On the bottom, click **Add person**.
14. Enter the Google Account email address and password, then click **Next**.
15. Follow the steps that appear.

Restrict Sign-in

16. Log back into the parent owner account.
17. Return to the **Manage other people screen**.
18. Toggle on (blue) **Restrict sign-in to the following users**.

Set up parental controls

Use Family Link  to turn on various parental controls. You can find step-by-step instructions on how to do this on page 92, *Setting up parental controls with Family Link*.


Add a school account for a Family Link user

Google Workspace for Education administrators determine which Google services their users (students) can access while signed into a Google Workspace for Education account. This may include some features or services that your child was previously unable to access using the Family Link supervised account.

A parent's Family Link parental controls will apply to a school account if:

- You're on a Chromebook with Chrome OS versions 83 and up. Learn more about how to update your Chromebook's operating system.
- Your child's personal Google account is managed by Family Link . Learn how to create a Google Account for your child.
- A school account is added as a secondary account.


Add a school account as a secondary account


1. On your Chromebook, sign in to your child's personal Google account managed by Family Link.
2. At the bottom right, click on the time area.
3. Select  Settings .
4. On the left, select **People**.
5. Select your child's personal Google account managed by Family Link.
6. Next to "Accounts," select **Add school account**.
7. Follow the on-screen steps. To approve the addition of a school account, a parent will need to give permission.

Important: If you add a school account as a new user on your Chromebook's sign-in screen, Family Link parental controls will not apply to that user account.

Remove a school account as a secondary account

On your Chromebook, sign in to your child's personal Google account managed by Family Link.

1. At the bottom right, select the time area.
2. Select  Settings .
3. On the left, select **People**.
4. Select your child's personal Google account managed by Family Link.

5. Next to the school account you want to remove, select **More** .
6. Select **Remove this account**. A parent will need to give permission to remove a school account.

How Family Link works with a school account

Screen time limits, bedtimes, and other parental controls apply whenever a child is signed in to a Chromebook with their Family Link account. Adding a school account for a Family Link user lets the child use school apps like Google Classroom while the same parental controls apply.

When a school account is added as a secondary account for a Family Link user, a child can:

- Switch between accounts to check email.
- Switch between accounts while on some Chrome Web Store extensions and Android apps, like Google Classroom, to do schoolwork under parent supervision.
- Sign in to websites using a school account.

Block Porn & Unsafe Websites



I recommend you use a layered security approach to your child's online safety. We need a reliable solution to address the different ways your child will be connecting to the Internet. Your child will be connecting through your home Wi-Fi, their phone's data plan, and any other available Wi-Fi connection they may find. Based on these requirements, I have discovered CleanBrowsing.org as a free one-stop solution. Their DNS filters can be used on your router and all your child's devices.

CleanBrowsing is a DNS-based filter that prevents adult content from being loaded. It doesn't require any software installation and can be easily enabled anywhere by switching your DNS servers to the ones they provide. They also offer Apps for major devices to simplify installation. CleanBrowsing has three free content filters available via IPv4 and IPv6. Choose the one that fits your needs the most.

Family Filter

Blocks access to all adult, pornographic and explicit sites. It also blocks proxy and VPN domains that are used to bypass the filters. Mixed content sites (like Reddit) are also blocked. Google, Bing, and YouTube are set to the Safe Mode. Malicious and Phishing domains are blocked.

IPv4 address: **185.228.168.168** and **185.228.169.168**

IPv6 address: **2a0d:2a00:1::** and **2a0d:2a00:2::**

Adult Filter

Blocks access to all adult, pornographic and explicit sites. It does not block proxy or VPNs, nor mixed-content sites. Sites like Reddit are allowed. Google and Bing are set to the Safe Mode. Malicious and Phishing domains are blocked.

IPv4 address: **185.228.168.10** and **185.228.169.11**

IPv6 address: **2a0d:2a00:1::1** and **2a0d:2a00:2::1**

Security Filter

Blocks access to Phishing, spam, malware, and malicious domains. Our malicious domain database is updated hourly and considered to be one of the best in the industry. Note that it does not block adult content.

IPv4 address: **185.228.168.9** and **185.228.169.9**

IPv6 address: **2a0d:2a00:1::2** and **2a0d:2a00:2::2**

Windows OS

The easiest way to install CleanBrowsing on your Windows device is to use their App. It saves time and avoids some of the more common mistakes users make when configuring DNS manually.

Download the App here: <https://cleanbrowsing.org/guides/windows>

macOS

Install CleanBrowsing on your Mac by using their App. Download the App here: <https://cleanbrowsing.org/guides/macOS>

iOS (iPhone & iPad)

The iPhone doesn't have a straightforward way to change the DNS servers. I recommend using their free App. Go to the App Store, search for CleanBrowsing and install it.

Android OS

Use the official CleanBrowsing Android App, available in the Google Play Store, to set up CleanBrowsing on your Android device. Go to the Google Play Store, search for CleanBrowsing and install it.

CleanBrowsing also has paid plans that allow enhanced features such as custom block pages, additional categories, and logging and visibility.

Your Router

You are responsible for every person/device that connects to the Internet through your Wi-Fi (i.e., guest, kid's friends, babysitter, visiting family, etc.) Your Wi-Fi router should also have content filtering. You have two choices:

One, you can use a router that has content filtering built-in. Many new Wi-Fi routers have parental controls and filtering; however, they do not all have the same level of effectiveness or ease of use. If you choose to purchase a Wi-Fi router, I recommend the Gryphon Mesh Wi-Fi Security Router & Parental Control System.

Two, you can configure your current router to use CleanBrowsing's DNS filters. This will require a little more tech-savviness. CleanBrowsing does have installation help documents on standard routers here: <https://community.cleanbrowsing.org/article-categories/routers-network-devices/>

Parent Monitoring & Notification App



Bark - Parental Controls (iPhone and Android)

Bark provides families with the tools they need to raise kids in the digital world. Their comprehensive service lets you monitor content, manage screen time, and filter websites so you can get peace of mind while your child is online. Bark has won awards from The National Parenting Center, Mom's Choice Awards, and National Parenting Product Awards.

Bark uses advanced algorithms to detect and proactively alert parents to issues their children face online, such as cyberbullying, sexting, and signs of depression and suicidal thoughts. Bark covers text messaging, YouTube, email, and social media platforms and apps — 4x more than any other child monitoring app. You'll get automatic alerts to signs of cyberbullying, depression, online predators, adult content, and more. By only showing parents potential problems, Bark's approach saves parents valuable time and helps build trust between parent and child.



Content Monitoring

Bark monitors your child's texts, email, YouTube, and 30+ apps and social media platforms for issues like cyberbullying, adult content, sexual predators, profanity, suicidal ideation, threats of violence, and more. Parents receive alerts only when something potentially problematic occurs online. You won't have full access to everything on your child's phone — just the things you might need to know about.

Screen Time Management

Families can set healthy time limits and create schedules for when their children's devices can connect to the internet (through both cell service and Wi-Fi).

Web Filtering

Our web filter lets you select which websites your child can access on their devices. You can allow or block specific sites — or even whole categories like streaming services, online gaming, sexual content, and more.

We are proud to partner with Bark to give you a 15% discount on your paid subscription. Use our promo-code, **cybersafetycop**, when you sign up.

Parent Presentation



Based on Clay Cranford's acclaimed book, *Parenting in the Digital World*, this 90-minute cyber safety seminar will prepare parents to effectively supervise their child on social media sites, protect them from online threats, and bring technological balance back to their homes.

In this "new normal" where children are learning online from home, they are exposed more than ever to online predators and the damaging effects of screen time. This seminar will show you the current games, and apps teens are using today. Secondly, cyberbullying and other online threats are defined with current trends and real-world examples that Clay Cranford has investigated in schools. Lastly, participants will be given tools and an action plan that they can immediately begin using to help keep their children safe online.

Topics Include

- Current apps kids are using and what you need to know about them
- "Sexting" and online predators
- How to talk to your child about online safety
- How to monitor online activity and find secret Instagram accounts
- How to talk to your child about pornography
- Parental controls and privacy settings



What educators and parents are saying about the Cyber Safety Cop assembly...



"Every parent should be required to attend his presentation! I learned so much in the two hours there and walked away feeling more informed and confident in having a solid game plan to protect my kids."

Nani L. - Parent

The best parent night we have had in my 29 years as an educator.

Michelle B. - Middle School Principal

Contact the Cyber Safety Cop team through our website, www.cybersafetycop.com, to find out how to bring this eye-opening presentation to your school.

Student Presentations

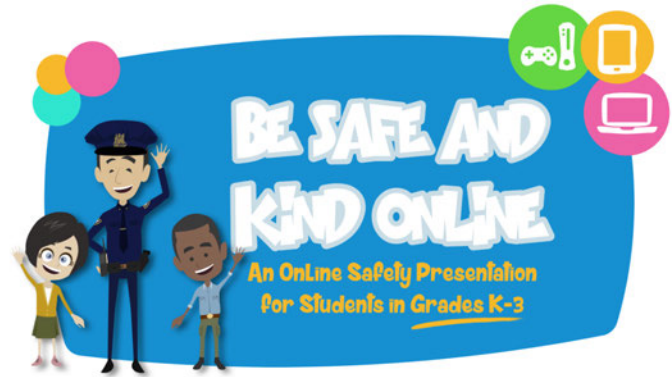


Clayton Cranford, the founder of Cyber Safety Cop, and his instructors travel throughout the United States and share their cyber safety message with tens of thousands of students, Kindergarten through 12th grade. Our 40-minute presentation is typically taught in a large assembly format but can be taught to small groups or even via webinars.

Our presentations get schools CIPA compliant. Schools and libraries subject to the Children's Internet Protection Act must educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The Cyber Safety Cop assemblies satisfy the CIPA educational requirement.

Kindergarten - 3rd Grade "Be Safe and Kind Online"

Be Safe and Kind Online equips younger students with the skills and knowledge necessary to use the internet safely, creating an awareness of potential problems they may experience when they are online and how to manage these issues and ask for help. This is achieved through a dynamic, engaging, and non-scary presentation. The topics are introduced by animated characters that children can enjoy and relate to Zachary, Charlotte, and the Cyber Safety Cop.



Topics include:

- Telling a trusted adult when anything makes them feel sad, scared, or confused.
- Not sharing personal information with someone they meet online.
- Anti-cyberbullying strategies.

4th – 6th Grade

The 4th – 6th grade cyber safety assembly gives elementary students the information they need to make good decisions in their online lives. Through real-life experience as a juvenile investigator, the presenter will share common safety issues and how students can make themselves more secure in social networks. The program focuses on the importance of a positive Digital Reputation and the long-term impact of cyberbullying can have on their lives. Topics include:

- Not allowing strangers in your network.
- Consequences of mean, rude, or threatening messages
- How to create a positive online reputation.

7th – 12th Grade

The 7th – 12th grade cyber safety assembly builds off of the 4th – 6th assembly. The same topics are covered: Not allowing strangers in your network; and the consequences of mean, rude, or threatening messages. The presenter, a former juvenile investigator, will take the topics one step further and discuss:

- Online sexual exploitation and sexting.
- Criminal harassment and threats, and how to avoid making these mistakes.
- We end the presentation on how to create a positive online reputation.

What educators and parents are saying about the Cyber Safety Cop assembly...

“My oldest daughter was in your assembly yesterday for the first time. It was incredible to hear her share her perspective about what and how you explained the dynamics and dangers of the cyber world. My husband and I cannot begin to express the gratitude for what all you do for these kiddos/this generation and those that follow.”

Andi B. - Parent of a 5th Grade Student

“My 7th grader heard Clay Cranford, and his “Cyber Safety” talk at school. He came home and said, “Mom, I’m gonna take this technology and phone thing serious!” THANK YOU CLAY!!!! You hit home and are getting through to the kids!”

Amanda M. - Parent of a 7th Grade Student

“Thank you for your informative presentation. My seventh graders really enjoyed it. Some of them, on their way home from school on Friday, denied friend requests from people they didn't know. Another student was on his PlayStation over the weekend and was friended by someone he didn't know. He quickly quit the game. I think some of them have awoken from their slumber. They also really enjoyed hearing true stories such as the one with Cindy, the blonde 16-year-old girl. Thanks for making a difference.”

Sue H. - Middle School Teacher

Contact the Cyber Safety Cop team through our website, www.cybersafetycop.com, to find out how to bring this eye-opening presentation to your school.

References



When Should I Give My Child a Phone or Social Media?

1. Giedd, J.N. et al. October 1999. "Brain development during childhood and adolescence: a longitudinal MRI study." *Nature*. Vol 2, No 10, pp. 861-863.
2. *ibid*
3. Brownlee, S. August 9, 1999. "Inside the Teen Brain." *U.S.News*.

The Problem with Social Media

1. Internet Users. (n.d.). Retrieved August 9, 2017, from <http://www.internetlivestats.com/internet-users/>

Online Reputation & Privacy

1. Kaplan Test Prep Survey: Percentage of College Admissions Officers Who Check Out Applicants' Social Media Profiles Hits New High; Triggers Include Special Talents, Competitive Sabotage | Kaplan Test Prep. (2016). *Kaptest.com*. Retrieved 3 March 2020, from <https://www.kaptest.com/blog/press/2016/01/13/kaplan-test-prep-survey-percentage-of-college-admissions-officers-who-check-out-applicants-social-media-profiles-hits-new-high-triggers-include-special-talents-competitive-sabotage/>
2. Survey: 70 pct of job recruiters have rejected candidates for online profile content. (2014). *ABC7 Chicago*. Retrieved 3 March 2020, from <https://abc7chicago.com/careers/survey-70-pct-of-job-recruiters-have-rejected-candidates-for-online-profile-content/443496/>

Screen time

1. The Common Sense Census: Media Use by Tweens and Teens, [Accessed May 17] Available from: <https://www.common sense media.org/research/the-common-sense-census-media-use-by-tweens-and-teens>
2. Social media captures 30% of online time, [Accessed May 17] Available from: <http://blog.globalwebindex.net/chart-of-the-day/social-media-captures-30-of-online-time/>
3. Jenner, F. 2015. At least 5% of young people suffer symptoms of social media addiction. [Accessed Mar 17] Available from: https://horizon-magazine.eu/article/least-5-young-people-suffer-symptoms-social-media-addiction_en.html
4. Hofmann, W. Vohs, D. Baumeister, R. 2012. What people desire, feel conflicted about, and try to resist in everyday life. [Accessed April 17] Available from: <http://journals.sagepub.com/doi/full/10.1177/0956797612437426>
5. <https://www.cnn.com/2019/11/04/health/screen-time-lower-brain-development-preschoolers-wellness/index.html>

6. The Mental Health Foundation. 2004. Lifetime impacts: Childhood and adolescent mental health – understanding the lifetime impacts. [Accessed Apr 17] Available from: https://www.mentalhealth.org.uk/sites/default/files/lifetime_impacts.pdf
7. Sampasa-Kanyinga Hugues and Lewis Rosamund F.. *Cyberpsychology, Behavior, and Social Networking*. July 2015, 18(7): 380-385. doi:10.1089/cyber.2015.0055.
8. Anxiety.org. 2016. Compare and despair. [Accessed Mar 17] Available from: <https://www.anxiety.org/social-media-causes-anxiety>
9. Becker, M. Alzahabi, R. Hopwood, C. *Cyberpsychology, Behavior, and Social Networking*. February 2013, 16(2): 132-135. doi:10.1089/cyber.2012.0291.
10. Mind. How to cope with sleep problems. [Accessed Apr 17] Available from: <http://www.mind.org.uk/information-support/types-ofmental-health-problems/sleep-problems/>
11. National Institute of Mental Health. 2016. The teen brain: 6 things to know. [Accessed Apr 17] Available from: <https://www.nimh.nih.gov/health/publications/the-teen-brain-still-under-construction/index.shtml>
12. Blakemore, S.-J. and Choudhury, S. (2006), Development of the adolescent brain: implications for executive function and social cognition. *Journal of Child Psychology and Psychiatry*, 47: 296–312. doi:10.1111/j.1469-7610.2006.01611.x <http://onlinelibrary.wiley.com/doi/10.1111/j.1469-7610.2006.01611.x/full>
13. Scott, H. Gardani, M. Biello, S. Woods, H. 2016. Social media use, fear of missing out and sleep outcomes in adolescents. [Accessed Apr 17] Available from: https://www.researchgate.net/publication/308903222_Social_media_use_fear_of_missing_out_and_sleep_outcomes_in_adolescence
14. Harvard Health – Harvard Medical School. 2015. Blue light has a dark side. [Accessed Apr 17] Available from: <http://www.health.harvard.edu/staying-healthy/blue-light-has-a-dark-side>
15. Woods, H. Scott, H. 2016. #sleepyteens: Social media use in adolescence is associated with poor sleep quality, anxiety, depression and low self-esteem. *Journal of Adolescence* · August 2016 DOI: 10.1016/j.adolescence.2016.05.008
16. Lamb, B. 2015. *Human diversity: Its nature, extent, causes and effects on people*. Singapore. World Scientific Publishing.
17. Carolyn Edgecomb, Do's and Don'ts of Instagram: Take a Picture, It Reaches Further, [Accessed Mar 17] Available from: <https://www.impactbnd.com/dos-and-donts-of-instagram>
18. Fardouly, J. Diedrichs, P. C. Vartanian, L. Halliwell, E. 2015. Social comparisons on social media: The impact of Facebook on young womens body image concerns and mood. *Body Image*, 13. pp. 38-45. ISSN 1740-1445 Available from: <http://eprints.uwe.ac.uk/24574>
19. Holland, G., & Tiggemann, M. (2016). A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes. *BodyImage*, 17, 100-110. doi:10.1016/j.bodyim.2016.02.008
20. The British Association of Aesthetic Plastic Surgeons. 2016. 'Daddy Makeovers' and Celeb Confessions:

Cosmetic Surgery Procedures Soar in Britain. [Accessed Apr 17] Available from: <http://baaps.org.uk/about-us/>

21. UPMC/University of Pittsburgh Schools of the Health Sciences, Social Media Use Associated With Depression Among U.S. Young Adults, Accessed Mar 17] Available from: <http://www.upmc.com/media/NewsReleases/2016/Pages/lin-primack-sm-depression.aspx>

22. Computer/Internet Addiction Symptoms, Causes and Effects, [Accessed May 17] Available from: <http://www.psychguides.com/guides/computerinternet-addiction-symptoms-causes-and-effects/>

23. Hailey Middlebrook, New screen time rules for kids, by doctors, [Accessed May 17] Available from: <http://www.cnn.com/2016/10/21/health/screen-time-media-rules-children-aap/>

24. George Dvorsky, Kids Who Use Touchscreen Devices Sleep Less at Night, [Accessed Apr 17] Available from: <http://gizmodo.com/kids-who-use-touchscreen-devices-sleep-less-at-night-1794270842>

25. Elgar FJ, Napoletano A, Saul G, Dirks MA, Craig W, Poteat VP, Holt M, Koenig BW. Cyberbullying Victimization and Mental Health in Adolescents and the Moderating Role of Family Dinners. *JAMA Pediatr.* 2014;168(11):1015-1022. doi:10.1001/jamapediatrics.2014.1223

26. Rick Nauert PhD, Family Dinners Can Bolster Teens' Mental Health, [Accessed May 17] Available from: <https://psychcentral.com/news/2013/03/21/family-dinners-can-bolster-teens-mental-health/52849.html>

Online Sexual Exploitation

1. <http://www.dailymail.co.uk/news/article-2888300/Is-child-s-new-iPad-magnet-paedophiles-Ten-year-old-girl-groomed-tablet-perverts-despite-parents-taking-sensible-safety-measures.html>

2. "My story: Struggling, bullying, suicide, self harm," Available from: https://www.youtube.com/watch?time_continue=1&v=vOHXGNx-E7E&feature=emb_logo&bpctr=1583273917

3. Department of Homeland Security, "Blue Campaign: Human Trafficking 101," <http://www.dhs.gov/sites/default/files/publications/blue-campaign/bc-inf-ht101-blue-campaign-human-trafficking-101.pdf>

Sexting

1. Chances Are Your Teen is Sexting

Chances Are Your Teen is Sexting. (2021). Retrieved 3 February 2021, from <https://time.com/2948467/chances-are-your-teen-is-sexting/>

2. Madigan S, Ly A, Rash CL, Van Ouytsel J, Temple JR. Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatr.* 2018;172(4):327–335. doi:10.1001/jamapediatrics.2017.5314

3. Majority of Minors Engage in Sexting, Unaware of Harsh Legal Consequences - DrexelNow

Majority of Minors Engage in Sexting, Unaware of Harsh Legal Consequences - DrexelNow. (2021). Retrieved 3 February 2021, from <https://drexel.edu/now/archive/2014/June/Sexting-Study/>

How to Talk to Your Child About Pornography

1. Hilton, D. L., And Watts, C. (2011). Pornography Addiction: A Neuroscience Perspective. *Surgical Neurology International*, 2: 19; (<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3050060/>)
2. Hedges, V. L., Chakravarty, S., Nestler, E. J., And Meisel, R. L. (2009). Deltafosb Overexpression In The Nucleus Accumbens Enhances Sexual Reward In Female Syrian Hamsters. *Genes Brain And Behavior* 8, 4: 442–449;
3. Bostwick, J. M. And Bucci, J. E. (2008). Internet Sex Addiction Treated With Naltrexone. *Mayo Clinic Proceedings* 83, 2: 226–230;
4. Doidge, N. (2007). *The Brain That Changes Itself*. New York: Penguin Books, 106; Nestler, E. J. (2005). Is There A Common Molecular Pathway For Addiction? *Nature Neuroscience* 9, 11: 1445–1449.
5. Angres, D. H. And Bettinardi-Angres, K. (2008). The Disease Of Addiction: Origins, Treatment, And Recovery. *Disease-A-Month* 54: 696–721; Doidge, N. (2007). *The Brain That Changes Itself*. New York: Penguin Books, 102.
6. Pitchers, K. K., Vialou, V., Nestler, E. J., Laviolette, S. R., Lehman, M. N., And Coolen, L. M. (2013). Natural And Drug Rewards Act On Common Neural Plasticity Mechanisms With DeltaFosB As A Key Mediator. *Journal Of Neuroscience* 33, 8: 3434–3442;
7. Angres, D. H. And Bettinardi-Angres, K. (2008). The Disease Of Addiction: Origins, Treatment, And Recovery. *Disease-A-Month* 54: 696–721;
- Zillmann, D. (2000). Influence Of Unrestrained Access To Erotica On Adolescents' And Young Adults' Dispositions Toward Sexuality. *Journal Of Adolescent Health* 27, 2: 41–44.
8. Bridges, A. J. (2010). Pornography's Effect On Interpersonal Relationships. In J. Stoner And D. Hughes (Eds.) *The Social Costs Of Pornography: A Collection Of Papers* (Pp. 89–110). Princeton, NJ: Witherspoon Institute;
- Bergner, R. And Bridges, A. J. (2002). The Significance Of Heavy Pornography Involvement For Romantic Partners: Research And Clinical Implications. *Sex And Marital Therapy* 28, 3: 193–206.
9. Kristin Maxwell and James Check, "Adolescents' rape myth attitudes and acceptance of forced sexual intercourse." Paper presented at the Canadian Psychological Association Meetings, Quebec, June 1992.
10. Wildmom-White, M. L. And Young, J. S. (2002). Family-Of-Origin Characteristics Among Women Married To Sexually Addicted Men. *Sexual Addiction & Compulsivity* 9, 4: 263–73.
11. Wright, P. (2013). U.S. Males And Pornography, 1973–2010: Consumption, Predictors, Correlates. *Journal Of Sex Research* 50, 1: 60–71;
12. Dedmon, J. (2002). Is The Internet Bad For Your Marriage? Online Affairs, Pornographic Sites Playing Greater Role In Divorces. Press Release From The Dilenschneider Group, Inc.
13. Watson, Connie. "The Globalization of Sex." CBC News. CBC/Radio Canada, 18 June 2009. Web. 06 Jan. 2015.

14. Dines, Gail, and David Levy. "Good Cop Bad Cop: Corporate Political Strategy in the Porn Industry." Web log post. Organizations and Social Change. N.p., 13 Nov. 2013. Web.

15. Farley, M. "Renting an Organ for Ten Minutes: What Tricks Tell us about Prostitution, Pornography, and Trafficking." (2007)

Bullying

1. Rutgers University. "Teen girls more vulnerable to bullying than boys." ScienceDaily. ScienceDaily, 7 May 2019.

2. Bullying Definition. (2012, February 29). Retrieved August 06, 2017, from <https://www.stopbullying.gov/what-is-bullying/definition/index.html>

3. Idsoe, T., Dyregrov, A. & Idsoe, E.C. J Abnorm Child Psychol (2012) 40: 901. <https://doi.org/10.1007/s10802-012-9620-0>

Identity Theft and Hacking

1. Dalasta, D. (n.d.). Phishing Data – Attack Statistics. Retrieved August 13, 2017, from <http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-data-attack-statistics/#gref>

Internet & Mobile Device Usage Contract

1. National Crime Prevention Council, "Stop Bullying Before it Starts," <http://www.ncpc.org/resources/files/pdf/bullying/cyberbullying.pdf>

2. Harris Interactive, "Trends & Tudes 2007 Volume 6 Issue 4," April 2007

Popular Apps & Games

1. 10 sentenced to prison for child exploitation enterprise & conspiracy (2020). Retrieved 17 February 2021, <https://www.biometrica.com/10-sentenced-to-prison-for-child-exploitation-enterprise-conspiracy/>

2. Safety Principles and Policies I Discord. (2021). Retrieved 17 February 2021, from <https://discord.com/safety>

3. Family View - Steam Support . (2021). Retrieved 17 February 2021, from https://support.steampowered.com/kb_article.php?ref=5149-EOPC-9918

4. Home - Roblox. (2021). Retrieved 17 February 2021, from <https://corp.roblox.com/>

5. Parents' Ultimate Guide to Fortnite. (2020). Retrieved 17 February 2021, from <https://www.common sense media.org/blog/parents-ultimate-guide-to-fortnite>

6. Epic Games' Fortnite. (2021). Retrieved 17 February 2021, from <https://www.epicgames.com/fortnite/en-US/parental-controls>

7. Parents' Ultimate Guide to Minecraft. (2020). Retrieved 17 February 2021, from <https://www.common sense media.org/blog/parents-ultimate-guide-to-minecraft>

8. All about Pinterest (2021). Retrieved 17 February 2021, from <https://help.pinterest.com/en/guide/all-about->

pinterest

iPhone & iPad Parental Controls

<https://support.apple.com/en-us/HT201304>

How Children are Hacking iOS Screen Time

<https://www.washingtonpost.com/technology/2019/10/15/teens-find-circumventing-apples-parental-controls-is-childs-play/>

Android Parental Controls

<https://support.google.com/googleplay/answer/1075738?hl=en>Xbox Parental Controls

Xbox Parental Controls

<https://www.xbox.com/en-US/community/for-everyone/responsible-gaming>

Playstation 4 & 5 Parental Controls

<https://www.playstation.com/en-us/support/account/ps5-parental-controls-spending-limits/>

Nintendo Switch Parental Controls

<https://www.nintendo.com/switch/parental-controls/>

Windows 10 Parental Controls

<https://support.microsoft.com/en-us/account-billing/set-screen-time-limits-on-your-kids-devices-a593d725-fc4c-044c-284d-32eab0305ffd>

macOS Parental Controls

<https://support.apple.com/guide/mac-help/set-up-content-and-privacy-restrictions-mchl8490d51e/mac>

Chromebook Parental Controls

<https://support.google.com/families/answer/7087030?hl=en>

Block Porn & Unsafe Websites

<https://cleanbrowsing.org/content-filtering>

About the Author



CLAYTON CRANFORD IS The Cyber Safety Cop



Clayton Cranford is a law enforcement professional based in Southern California and owner of Total Safety Solutions. Clayton is one of the nation's leading law enforcement educators on social media and child safety. He created Cyber Safety Cop, an Internet and social media safety program. It teaches parents and students how to avoid the inherent risks of social media and other web based platforms by using safe habits.

Clayton has more than 20 years of teaching experience and has been a

featured speaker at the National Conference on Bullying, the Southwest Conference on Human Trafficking, the California Association of Crime Prevention Officers, and the National Association of School Resource Officers.

Clayton was awarded the 2015 National Bullying Prevention Award from the School Safety Advocacy Council, and the 2015 American Legion Medal of Merit for his bullying prevention work.

Clayton has served as a School Resource Officer to, a Juvenile Investigator, a member of a county-wide school threat assessment team, and directed his county's school anti-drug abuse program. Clayton also teaches threat assessment investigation to law enforcement agencies through out the United States.

Clayton has partnered with Agape International Missions (AIM), a leader in the fight against child sex trafficking in Cambodia. Clayton has served overseas with AIM in Cambodia's child sex trafficking epicenter and speaks at various Human Trafficking symposiums and conferences.

Clayton is married to Gretchen, and they have two boys, Zachary and Clay, who love the Internet and technology. Clayton has a Bachelor's Degree in Philosophy and a Master's Degree in Criminal Justice.

PARENTING IN THE DIGITAL WORLD

A STEP-BY-STEP GUIDE TO INTERNET SAFETY

THIRD EDITION

“This book answers the number one question parents of digital kids have today, ‘How Can I Keep My Child Safe Online?’ Parenting in a Digital World is an indispensable guide that should live on the nightstand of every parent raising kids today.”

—Diana Graber, Co-Founder, Cyberwise.org and Founder, CyberCivics.com

Parenting in the Digital World is an up-to-date guide containing all of the essential information parents need to create a safe environment for their children online.

Cyber Safety Cop’s founder, Clayton Cranford, will take you step-by-step through the hidden settings on all the most popular social media apps, operating systems, gaming consoles, and mobile devices.

Clayton Cranford is a law enforcement professional based in Southern California. Clayton’s experience as a juvenile investigator, school resource officer, threat assessor, and father of two teenaged boys has made him one of the nation’s leading law enforcement educators on social media and child safety.

Clayton has taken his extensive experience and created this manual for parents to address key safety issues in their child’s digital lives.

The third edition includes updated parental control guides on all the devices your child is using, and new chapters on critical online safety issues: How to talk to your child about pornography, sexting, cyberbullying, and how to create a culture of safety and accountability in your home.

