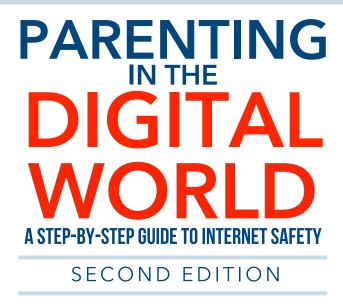
# 

A STEP-BY-STEP GUIDE TO INTERNET SAFETY



CLAYTON CRANFORD



## 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 from hereon out 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 978-1974552542

## Dedicated to My Family

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 indomitable wife, Gretchen, who has given me constant and unwavering support, our two boys, Clay and Zachary, who love technology and are my "goofballs," now and forever.

To my parents, Otis and Patricia who taught me to do good in the world, serve others, and be true to myself. To my two older brothers, Michael and Matthew, who introduced me to computers and technology when the Commodore 64 was state of the art. And my sister Kimberly, who's memory is a sweet presence in my life everyday.

And finally, this book is also dedicated to the parents, teachers, principals, law enforcement officers, and counselors who are dedicating themselves everyday to keeping our children safe. Thank you.



## Contents

Preface	1
Introduction	3
The Cyber Safety Cop Plan	5
Social Media Defined	6
Managing Your Online Reputation & Privacy	8
When Should I Give My Child Social Media?	10
Create Balance In Your Child's Technological Life	12
Online Predators Use Social Media to Exploit Children	20
How to Talk to Your Child About Pornography	25
Cyberbullying	31
Threats and Consequences	35
Internet & Mobile Device Usage Contract	37
Create Accountability	40
Protect Yourself From Getting Hacked	43
Popular Apps	45
App & Game Ratings	48
Parental Controls for Xbox 360	49
Parental Controls for Xbox One	51
Parental Controls for Playstation 4	53
Parental Controls for Windows 7	55
Parental Controls for Windows 8.1	57
Parental Controls for Windows 10	59
Parental Controls for Chromebook	64
Parental Controls for Mac OS	67
Parental Controls For iOS	69
Parental Controls For Android OS	71
YouTube Safe Search for Desktop	74
YouTube Safe Search for iOS	75
Google Safe Search for iOS and Desktop	76
Bing Safe Search	78
Yahoo Safe Search	79
Apple iMessage Privacy	80

Apple iMessage Monitoring	82
Instagram Privacy Settings & Reporting Abuse	84
Twitter Privacy & Security Settings Desktop and iOS	85
Facebook Privacy Settings	87
Facebook Privacy Settings Desktop Browser	88
Facebook Blocking Abuse	90
Facebook App Sharing Settings Desktop and iOS	92
Facebook Messenger Blocking iOS	93
Cyber Safety Cop Class Information	95
About the Author	96





### Preface

Thank you for purchasing the second edition to my book, Parenting in the Digital World. It has been two years since I published the first 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.

An unfiltered, unsupervised internet is one of the most dangerous places for our children to be.

"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 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

#### **EDUCATE YOURSELF**

- Go to a Cyber Safety Cop Parent Seminar (Page 95)
- Subscribe to the Cyber Safety Cop Newsletter (www.CyberSafetyCop.com)
- Review games and apps before you download them for your child at www.commonsensemedia.org

#### TALK WITH YOUR CHILD

- Use Internet Usage Contract (Page 37)
- Talk about your safety concerns
- Be open and direct

#### USE PARENTAL CONTROLS

- Follow the directions in this guide to activate the safety settings in your operating systems, search engines, and games
- Setup website filtering on your home network using www.opendns.com

#### SET RULES AND EXPECTATIONS

- Respect age limits on social media (Page 45)
- Enforce consequences when appropriate
- Charge your child's devices in your room at night

#### **ACCOUNTABILITY**

- Know all of your child's user names and passwords to all of their accounts
- Log into your child's social media accounts as them to monitor activity
- Periodically physically review the content on your child's device
- Install a monitoring/filtering application on your child's device

#### CREATE BALANCE

- Establish "screen time" limits for school nights and for weekends (Page 12)
- Plan family time without electronics
- Curb your own bad digital habits



### Social Media Defined

When you think of social media, I am willing to guess that Facebook and Instagram first come to mind. If we only look at Facebook and Instagram, two of the most popular social media platforms in the world, we will draw too narrow a definition and miss all the other places children communicate.

A broader, more inclusive definition of social media should be:

Social Media is any device or application that allows a user to communicate with another person.

This new definition of social media will hopefully open your eyes to a much bigger world. These devices and applications are really just portals to other people. The portal may be a web cam chat room with strangers or something as innocuous as Words with Friends. For parents to properly monitor their children's social networks, they must first realize that social media does not only exist on smart phones, tablets, and computers but exists in a whole new world of social networking that is constantly being created and expanded.

The Problem with Social Media

Social media and socially embedded technology are moving targets. Today's hot social media app could be easily replaced tomorrow with a new competitor.

After investigating cyberbullying and other social media related crimes over the years, I have traced the root of all the threats on social networks to two basic problems inherent in nearly all social media platforms.

- Children can communicate and meet people outside their parent's sphere of influence and control.
- Children and adults can communicate anonymously without any accountability, removing the natural inhibition or fear of getting caught.

Today's teens are sitting in their rooms with mobile devices in their hands. They have the Internet and 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.<sup>1</sup> An unsupervised, unfiltered Internet will leave a child open and vulnerable to threats and attacks that the parent and child are completely unprepared for.

Now that you understand what the two basic problems with social media are, you will look at the Internet in a new and completely different way. You will quickly see how a social network's privacy setting, or lack thereof, can allow strangers into your child's life. New social media applications are being created daily. Developers are looking for the next big thing. They are pushing the boundaries. They are trying to entice teens by creating new and exciting online experiences. Often, these new, exciting environments are not safe.

#### **Action Plan**

- 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?

#### **Notes**

1. Internet Users. (n.d.). Retrieved August 9, 2017, from http://www.internetlivestats.com/internet-users/

## Managing Your 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.

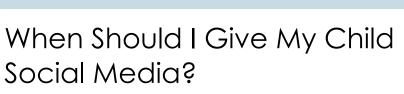
#### Privacy

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.

#### **Action Plan**

- Make sure each one of your child's social media accounts has a privacy setting and set to "private."
- Explain why it is dangerous to have people you don't know in your social network.
- Ask your child, "What's the upside to keeping a total stranger in your network?"
   Follow up with, "Do more likes make you a more popular person? Does it make you feel better about yourself? Should it?"
- Review each follower with your child.
- If your child does not have a real life face-to-face relationship with a "friend" or follower, then they must be removed or blocked. All new requests should only be granted to people your child has met in real life and can vouch for.





Possibly the most common question I get 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 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

Any child who has Facebook or Instagram knows the minimum age to have an account is thirteen. If a parent allows a child to have social media before the minimum age, they aren't fooling anyone. What kind of message are we sending to our children if we click "Agree" to the User Agreement when it clearly states the rule is no users under thirteen?" 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, but 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. 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. 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.<sup>3</sup> 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 time your teenager says, "I'm old enough to make my own decisions," you have the scientific authority and backing to say, "No you are not!" Case closed.

#### **Action Plan**

- 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.

#### **Notes**

- 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.



## Create Balance in Your Child's Technological Life

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

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.

What are the potential negative effects of social media on health?

#### 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.<sup>5</sup> 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).<sup>6</sup> 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.<sup>7</sup> Use of social media, particularly operating multiple social media accounts simultaneously, has also been shown to be linked with symptoms of social anxiety.<sup>8</sup>

#### 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.<sup>9</sup> Ask any parent of a newborn. The necessity of quality sleep is essential for everyone but is critical for teens and their brain development.<sup>10</sup> 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.<sup>11</sup> A growing number of studies have shown that increased social media use has a significant association with poor sleep quality in young people.<sup>12</sup> 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.<sup>13</sup> The lack of sleep and emotional investment in social media have also resulted in exasperating feelings of anxiety, depression, and lower self-esteem.<sup>14</sup>

#### 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. 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. 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. 17

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.<sup>18</sup> 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.<sup>19</sup> 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.<sup>20</sup> 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.<sup>21</sup>

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.<sup>22</sup>

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.<sup>23</sup>

Mobile apps like Parental Board by 4parents.com 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.<sup>24</sup>

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?"<sup>25</sup>

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) and 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 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, 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.

#### **Notes**

- The Common Sense Census: Media Use by Tweens and Teens, [Accessed May 17] Available from: https://www.commonsensemedia.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
- 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. 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
- 6. Sampasa-Kanyinga Hugues and Lewis Rosamund F.. Cyberpsychology, Behavior, and Social Networking. July 2015, 18(7): 380-385. doi:10.1089/cyber.2015.0055.
- 7. Anxiety.org. 2016. Compare and despair. [Accessed Mar 17] Available from: https://www.anxiety.org/social-media-causes-anxiety
- 8. Becker, M. Alzahabi, R. Hopwood, C. Cyberpsychology, Behavior, and Social Networking. February 2013, 16(2): 132-135. doi:10.1089/cyber.2012.0291.
- 9. 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/
- 10. 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
- 11. 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
- 12. 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
- 13. 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
- 14. 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
- 15. Lamb, B. 2015. Human diversity: Its nature, extent, causes and effects on people. Singapore. World Scientific Publishing.
- 16. 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
- 17. 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
- 18. 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. Bodylmage, 17, 100-110. doi:10.1016/j.bodyim.2016.02.008
- 19. 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/
- 20. 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
- 21. Computer/Internet Addiction Symptoms, Causes and Effects, [Accessed May 17] Available from: http://www.psychguides.com/guides/computerinternet-addiction-symptoms-causes-and-effects/
- 22. 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/
- 23. 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
- 24. 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
- 25. 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 Predators Use Social Media to Exploit Children



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.<sup>1</sup>

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.

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 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. Backpage is a popular online classified

Our social media connected teen is ... exposed to roughly 3.5 billion people on the Internet.

ads website, second only to Craigslist. A young girl, looking to get "discovered" as a model or musical talent, may respond to one of many ads on Backpage 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:

- 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.
- 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.
- 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.
- 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.

#### How Do I Identify 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.<sup>2</sup> 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:

http://www.dhs.gov/xlibrary/training/dhs\_awareness\_training\_fy12/launchPage.htm

#### **Notes**

- 1. http://www.dailymail.co.uk/news/article-2888300/ls-child-s-new-iPad-magnet-paedophiles-Ten-year-old-girl-groomed-tablet-perverts-despite-parents-taking-sensible-safety-measures.html
- 2. 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

## How to Talk to Your Child About Pornography



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.

Waiting to address this issue until after your child is exposed to pornography can be heart breaking. I have spoken to parents from all over the United States, and they have shared with me the personal agony they experienced when they discovered their child had already been exposed to online pornography. Sometimes this exposure was unintentional, and sometimes their child was seeking it out. Their stories are all so similar. They are shocked at how easy it was for their eight-year-old to land on a hardcore pornographic site accidentally, how disturbing and extreme the sex acts portrayed on the homepage of the website were, and collectively experience a strong sense of guilt and failure of not better protecting their child.

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." 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.<sup>2</sup> 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).<sup>3</sup> These chemicals are what make us feel happy and euphoric. Unfortunately, they can be hijacked by street drugs and pornography.<sup>4</sup>

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.<sup>5</sup> 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.<sup>6</sup> 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.<sup>7</sup>

#### 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.<sup>8</sup> 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.<sup>9</sup>

#### 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.<sup>10</sup> Studies have found that married porn users are more likely than non-users to have sex with someone other than their spouse.<sup>11</sup>

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. <sup>12</sup>

#### 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.<sup>13</sup> 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."<sup>14</sup>

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.<sup>15</sup>

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

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.

#### Notes

- 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/)
  - Bostwick, J. M. And Bucci, J. E. (2008). Internet Sex Addiction Treated With Naltrexone. Mayo Clinic Proceedings 83, 2: 226–230;
  - Nestler, E. J. (2005). Is There A Common Molecular Pathway For Addiction? Nature Neuroscience 9, 11: 1445–1449; Leshner, A. (1997). Addiction Is A Brain Disease And It Matters. Science 278: 45–7.
- 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;
  - Bostwick, J. M. And Bucci, J. E. (2008). Internet Sex Addiction Treated With Naltrexone. Mayo Clinic Proceedings 83, 2: 226–230;
  - Doidge, N. (2007). The Brain That Changes Itself. New York: Penguin Books, 108; Mick, T. M. And Hollander, E. (2006). Impulsive-Compulsive Sexual Behavior. Cns Spectrums, 11(12):944-955;
  - Nestler, E. J. (2005). Is There A Common Molecular Pathway For Addiction? Nature Neuroscience 9, 11: 1445–1449; Leshner, A. (1997). Addiction Is A Brain Disease And It Matters. Science 278: 45–7.
- 3. Bostwick, J. M. And Bucci, J. E. (2008). Internet Sex Addiction Treated With Naltrexone. Mayo Clinic Proceedings 83, 2: 226–230;
  - Balfour, M. E., Yu, L., And Coolen, L. M. (2004). Sexual Behavior And Sex-Associated Environmental Cues Activate The Mesolimbic System In Male Rats. Neuropsychopharmacology 29, 4:718–730;
  - Leshner, A. (1997). Addiction Is A Brain Disease And It Matters. Science 278: 45-7.
- 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;
  - 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, 105; Paul, P. (2007). Pornified: How Pornography Is Transforming Our Lives, Our Relationships, And Our Families. New York: Henry Hold And Co., 75.

- 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;
  - Zillmann, D. And Bryant, J. (1988). Effects Of Prolonged Consumption Of Pornography On Family Values. Journal Of Family Issues 9: 518–554.
- 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)



## 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, "Carliewhorebitchslutugly," 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.<sup>1</sup>

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.<sup>2</sup> 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 offical 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.

#### **Notes**

<sup>1.</sup> Bullying Definition. (2012, February 29). Retrieved August 06, 2017, from https://www.stopbullying.gov/what-is-bullying/definition/index.html

<sup>2.</sup> Idsoe, T., Dyregrov, A. & Idsoe, E.C. J Abnorm Child Psychol (2012) 40: 901. https://doi.org/10.1007/s10802-012-9620-0



# Threats and Consequences

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.

# 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. 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 1 in 10 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

### **Notes**

1. National Crime Prevention Council, "Stop Bullying Before it Starts," http://www.ncpc.org/resources/files/pdf/bullying/cyberbullying.pdf

# 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	Signature of parent	Date
After signing, post visibly by computer			



# 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

### 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.



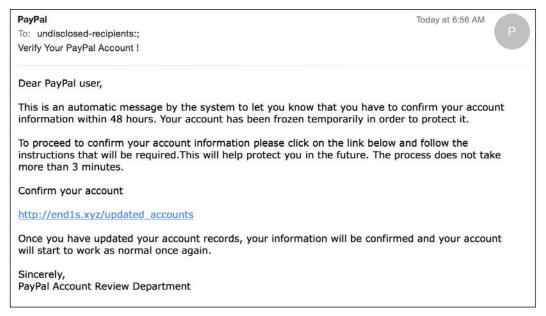




When we give our children an email account, social media, and access to the internet, they become vulnerable to online scams and identity theft. Children and the elderly are a rapidly growing segment of online fraud victims.

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.<sup>1</sup>

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:

- 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 "ransome-ware." It is a program that locks up the contents of your computer and can only be unlocked if your 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.

N	loi	عطا
1		L C 3.3

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









**Snapchat** (13+) 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. **Problem:** This app gives the sender the impression that they can send a "snap" without a care or concern to the possible 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. Additionally, teens might be using this app to hide conversations from their parents. Not safe for children.



**Kik Messenger** (+17) This instant messaging app is wildly popular among teens because it is a free cross platform app (it can be installed on just about any device, e.g., iPhone, iPod Touch, iPad, Android, or Windows phone). Your child doesn't need a cell phone service to use it. They only need WiFi. When teens send messages to their friends, they call it "kik'ing" a friend. **Problem:** A Kik user can create an account name that is not associated with a phone number, making authenticating a user's identity difficult. It also contains adult apps and content. Similar app: *TextNow or WhatsApp*. Not safe for children.



**Tinder** (+17) This app's primary purpose is to facilitate hooking-up and dating. 450 million profiles are rated every day. Tinder utilizes GPS location tracking to find people (strangers) near you. 13-17 year-olds now represent over 7 percent of the users on Tinder. **Problem:** Tinder makes it easy for your child to meet a complete stranger, possibly an adult, within walking distance. It also links to Instagram and Facebook. Similar apps: *Blender and Grinder*. Not safe for children.



**Whisper** (+17) This app allows the user to overlay an image with text to express their feelings anonymously. It does however display the area you are posting from and also allows the user to search for others posting near you. **Problem:** The anonymous nature of this app makes it ripe for cyberbullying. A user can post a picture of a fellow student and overlay derogatory text anonymously, a common tactic used by cyberbullies. The use of GPS to communicate with strangers nearby is very troubling. Similar app: *Secret*. Not safe for children.



**Yellow** (13+) is an app that describes itself as "a new social to make new friends and spend time with them with chat and live videos." Yellow does much more than that, it is the Tinder for teens: an app that allows teens to meet strangers and indicate if they are interested in meeting them in person. Not safe for children.



**Ask.fm** (+13) This App allows users to anonymously ask or answer other user's questions. **Problem:** There are many documented cases of cyberbullying on Ask.fm that have lead to suicide. Not safe for children.



Yik Yak (17+) Yik Kak is an app that allows users to post text-only (at least presently) messages, know as "Yaks," of up to 200 characters. The messages are viewed by the closest 500 Yakkers to the person who wrote the Yak. Yik Yak users are grouped together by their device's GPS location services. **Problem:** Yik Yak users are essentially anonymous. Yik Yak has been used to bully and threaten students. Not safe for children.



Omegle (13+) Omegle is a free online chat website that allows users to communicate with strangers without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the handles "You" and "Stranger." Problem: Omegle has a video chat that is not monitored for sexual content. The anonymous nature of this app has been known to attract pedophiles that want to expose themselves to children or interact with a minor that they have already groomed. Not safe for children.



**Fake Calculator** (No age) Fake Calculator is a "vault" app. Vault apps appear to work as advertised (a game or utility app), but in actuality they are used to hide pictures, files, and other apps inside of them; hence the name "vault" app. Similar apps: *Vault-Hide, NQ Vault, App Lock, Vaulty, Hide it Pro, and Personal.* Not safe for children.



**Twitter** (13+) This app is a social broadcast network that enables people and organizations to publicly share brief messages (140 characters per post) instantly around the world. Each post is referred to as a "tweet." **Problem:** Users can be bullied through replies, a embarrassing tweet can be shared and quickly go viral, no filtering of adult content, and children on Twitter can be contacted by adults. Use with caution.



**Facebook** (13+) Facebook is the most popular social network in the world. Users share posts/video/photos. Facebook offers apps, games, text and video chat. **Problem:** Without supervision and proper privacy settings, children are potential victims of bullying, and sexual victimization by adults. Use with caution.



Antichat (13+) Anticht is an anonymous chartroom platform. **Problem:** Antichat's anonymity encourages risk taking and accountability free behavior that often brings out the worst in people. A brief search of the public chartrooms finds very adult themed discussions and sexual predatory behavior. Not safe for children.



**YouTube** (13+) YouTube is the worlds largest video sharing site. Users can upload their own videos. **Problem:** People can comment on other's videos, resulting in cases of cyberbullying. Privacy settings are confusing and without proper content filtering, children can be exposed to inappropriate content. Use with caution.



**Skype** (13+) This app is one of the most popular video chatting and multiple communications platforms in the world. It is primarily used as a video chat platform. **Problem:** Without close adult supervision, children could have video chats with strangers they met on other sites. Use with caution.



**Tumblr** (17+) This app is a cross between a blog and Twitter. **Problem:** A user's first Tumblr account is public, open to anyone to read. Adult content can not be filtered. Not safe for children.



**Instagram** (13+) Instagram is the most popular image sharing social network for teens. **Problem:** Children can have adult followers. Cyberbullying through impersonation is relatively easy to do. Use with caution.



**Multi-Player Online Games** (varies; check rating) New multi-player games are being released daily for desktop computers and mobile devices. They allow the player to interact with other players in a virtual world. **Problem:** In app purchases can be very expensive. It is also very addictive. Children are playing with strangers, possibly adults. Similar games: Clash of Clans, World of Warcraft, & Wizard 101 Use with caution.



**Minecraft** (No age limit) Minecraft is a wildly popular world building game that allows online play with strangers or private group play. **Problem:** In-game chat can have swearing and bullying behavior. Use with caution.



**Periscope** (17+) Periscope is a live video streaming app that links to the user's Twitter account. **Problem:** Adult content is easily found on Periscope. Children who use Periscope can be seen by strangers and adults that can live text chat with them while on camera. Similar app: *Meerkat*. Not safe for children.



**WhatsApp** (13+) WhatsApp is an instant messaging app, similar to Kik Messenger. **Problem:** Users can be virtually anonymous. Cyberbullying and threats are difficult to trace back to the sender. Not safe for children.



House Party (4+) Houseparty is a group video chat app available on both apple and android devices. **Problem:** Unless the parent is sitting on their kid's shoulder, they will not know what is happening or being said on the video chat. The video chat is not recorded and cannot be reviewed later by the parent making accountability for children using this app very difficult. Use with caution.



**Facebook Messenger** (13+) This instant messaging app is linked to the user's Facebook account. **Problem:** Unsupervised messages can be used for bullying and sharing inappropriate images. Not safe for children.



**Pinterest** (13+) Pinterest is a social network to create digital bulletin boards and 'pin' images with links to the interesting things you find on the web to share with "friends" and "followers." **Problem:** Pinterest can link to Facebook and Twitter, causing privacy concerns. Use with caution.



**YouNow** (12+) YouNow is a live broadcasting platform. Users can make a live video or watch channels produced by others. **Problem:** YouNow does have rules against nudity and sexual content, but a live feed can't be prescreened or rated, so there's no real way to know what your teen will view next. Not safe for children.

Before allowing your child to download or install a game, carefully check its age rating, level of privacy, and parent reviews. You can find reviews for many social media applications on the blog page of www.cybersafetycop.com. I also recommend using parent focused review websites like Common Sense Media www.commonsensemedia.org.

The Entertainment Software Rating Board (ESRB) ratings provide guidance about video games and apps. www.esrb.org/ratings/



#### **EVERYONE**

Content is generally suitable for all ages. May contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language.



#### **EVERYONE 10+**

Content is generally suitable for ages 10 and up. May contain more cartoon, fantasy or mild violence, mild language and/or minimal suggestive themes.



#### **TEEN**

Content is generally suitable for ages 13 and up. May contain violence, suggestive themes, crude humor, minimal blood, simulated gambling and/or infrequent use of strong language.



#### **MATURE**

Content is generally suitable for ages 17 and up. May contain intense violence, blood and gore, sexual content and/or strong language.



#### **ADULTS ONLY**

Content suitable only for adults ages 18 and up. May include prolonged scenes of intense violence, graphic sexual content and/or gambling with real currency.



#### **RATING PENDING**

Not yet assigned a final ESRB rating. Appears only in advertising, marketing and promotional materials. It should be replaced by a game's rating once it has been assigned.





# Parental Controls for Xbox 360

The Xbox 360 console lets you customize and manage your family's access to games, movies, and television content. The Xbox 360 parental controls can be used to control both the console itself and access to content on Xbox Live.

- 1. On your console, go to **Settings**, and then select **Family**.
- 2. Select Content Controls.
- 3. Change settings to **On**. If you have set a passcode on this console before, you will enter it now. If you have not set a passcode, you will be prompted to set one now.

The console will provide you with preselected content settings. You can make changes to these settings on the menu items below.

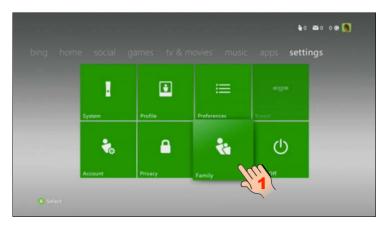
 I highly recommend setting up the Family Timer to help enforce screen time.

Select whether you want to set a **Daily** or **Weekly timer**.

Move down to the time period and use the left stick to increase or decrease the time period, then select **Continue**.

#### Select Save and Exit.

When the Family Timer is on, notifications will appear 1 hour, 30 minutes, 15 minutes, and 5 minutes before the time runs out. These give players sufficient warning so that they can save their games. However, when one of these notifications appears, you can add time or disable the timer altogether by entering your passcode.







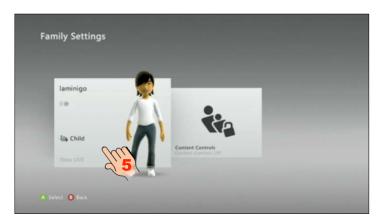
# Parental Controls for Xbox 360 continued

- 5. Click your child's account.
- Click on the right panel, Privacy & Online Settings. Select Change Settings.
- Select a preset option for your child's appropriate age, Teen, Child, or Customize.

**Child** will be the most strict security and privacy setting, blocking and filtering everything except online gameplay under the Activities menu. This is a good start.

**Teen** setting allows online gameplay and web browsing.

8. If you choose **Customize**, you can make discrete changes to the privacy and online settings.





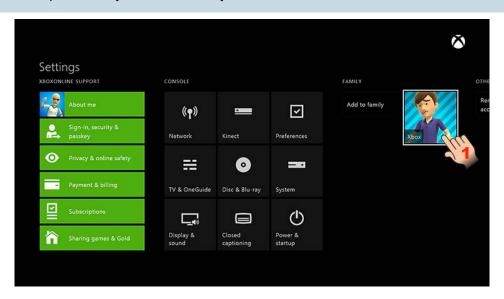




# Parental Controls for Xbox One

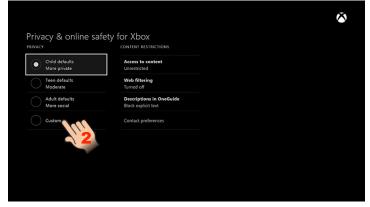
When managing a child's account, privacy and online safety together make up what are called "Parental controls." These settings should be applied to the Microsoft account of each individual child, allowing parents to customize the Xbox One experience for each of their children. To start managing a child's privacy and safety settings, follow these steps:

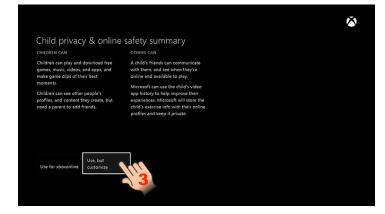
1. Sign in to your console. On your controller, press the **Menu** button. Select **Settings**. Scroll right to Family, then select the child profile that you want to modify.



- 2. After you select your child's profile, you're shown the current privacy settings and content restrictions for that child. Select any default privacy setting to see its definition. You can keep the default setting as is, or you can customize it.
- 3. To customize a setting, select **Use**, **but customize**.

You're presented with various customization options for each setting. Choose the options that best meet your family's online safety and privacy needs.





# Parental Controls for Xbox One continued

To view and customize the content restriction settings for your child, Press **B** on your controller to return to the previous screen.

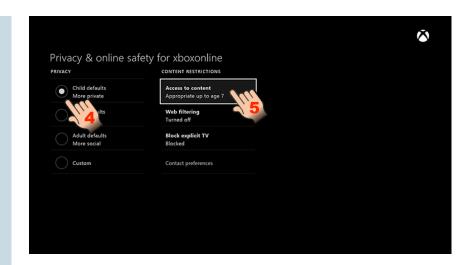
- 4. Select a setting to find out more about it.
- Select Access to content and apps to open a menu that will show you the details of your child's current content restrictions.

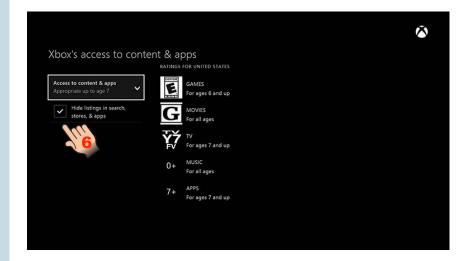
Select the level of restriction that's appropriate for your child. (Teen or Child)

By default, the level of restriction you set for your child is applied to searches, the store, and apps.

 (Optional) To remove this restriction, clear the check box next to Hide listing in search, stores, & apps.

The restriction will be removed for search, stores, and apps, but it will still be applied to actual content. When you're finished, press **B** on your controller to return to the previous screen.





## View and customize the web filtering settings for your child

Web filtering lets you choose the kinds of websites your child can visit using Internet Explorer. To set a web filtering level for your child:

- 1. On your controller, press the **Menu** button.
- 2. Select **Settings**.
- 3. Select your child's profile.
- 4. Under Content Restrictions, select Web filtering.
- 5. Here, you'll see a menu that enables you to select the level of filtering that's appropriate for your child.
- 6. When you're finished, press **B** on your controller to return to the previous screen.







To get the most of out the PS4's parental controls, you will want to make sure the adult has a Master Account, and the minor has a Sub Account. The Master Account controls what is and isn't accessible to Sub Accounts, and different rules can be created for individual Sub Accounts.

Creating A Sub Account for your child

# 1-2. Go to Settings icon ➤ Parental Controls ➤ Sub Account Management

You will now be asked to verify your PSN account by entering in your Sign-In ID (Email Address) and Password. Next, select **Create New Sub Account**, and press the  $\bigotimes$  button icon. Read the explanation of Sub Accounts. Then, select **next** and press the  $\bigotimes$  icon button. Select your child's Local User icon profile or click [Register User] to create a new local user profile. Then press the  $\bigotimes$  icon button. On the next screen, enter the Language and Date of Birth, and press the  $\bigotimes$  icon button.

Chat: The default setting is "Block" meaning chat is restricted. Sub Account holders will not be able to participate in text or voice / video chat with other PlayStation Network users.

Content Restriction: The default value is set to "On" meaning content will be restricted based on user age. If this restriction is removed, Sub Accounts will be able to buy and play any content, including content that is rated higher than their age, or is inappropriate for their age according to the ESRB rating system.





# Parental Controls for PS4 continued

 Return to the Parental Controls menu, and select Restrict Use of PS4 Features.

In order to use these features, you'll need a 4-digit passcode. By default, the code is "0000," but you can alter it by choosing **Change**Passcode.

 You can restrict games based on different levels on a scale of 1 to 11.

**Level 1** is for games that have not yet been rated.

**Level 2** allows only EC-rated (Early Childhood) games.

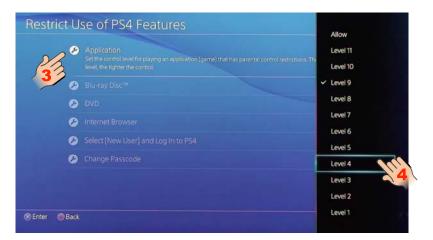
Level 3 allows E (Everyone),

**Level 4** allows E10+ (Everyone age 10 and up),

Level 5 to 8 allows Teen

**Level 9** allows Mature. The system is set to 9 by default.

- You can also set the age limits for Blu-Ray and DVD movies under Blu-Ray Disc and DVD respectively.
- 6. Turn off Internet Browsing under Internet Browser
- 7. Block others from creating new users on your console under Select [New User] and log in to PS4.













- Open Control Panel and click on Set up parental controls for any user.
- 2. Create or click on the child's account you want to set up

Make sure to password protect your Administrator account, otherwise your child can turn off Parental Controls and use the computer without restrictions.

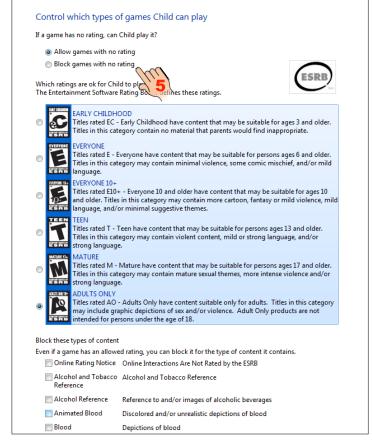
- 3. Under Parental Controls mark the radio button next to **On, enforce current settings**.
- 4. Then you can go through and control their computer time, games, and programs.

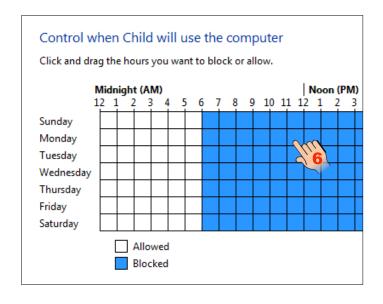


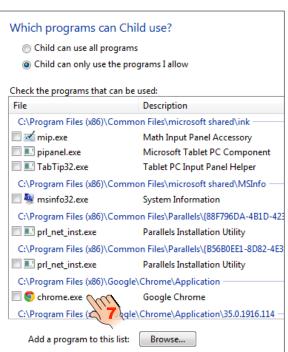


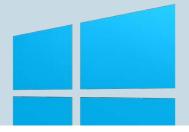


- Click on **Games** to set the ratings your child will be allowed to play.
- Click on **Time limits** to control when your child has access to the computer.
- Click Allow and block specific program to choose only the programs you want your child to use.







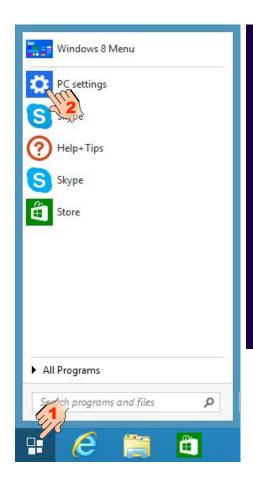




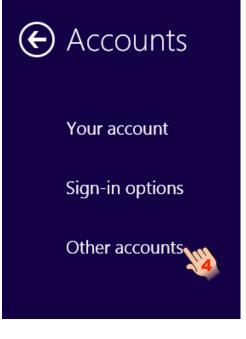


Family safety is the security feature within Windows 8.1 that provides control over your children while the using PC. Family safety provides web filtering, time limits, application and game restrictions and control over website accessing. You can apply family safety in Windows to existing child account or to a new account.

- 1. Sign in to your PC with the administration account.
- 2. Click Start menu, click on drop down menu and select PC settings.
- 3. Select Accounts.
- 4. Other Account.

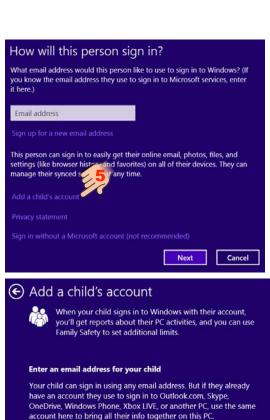


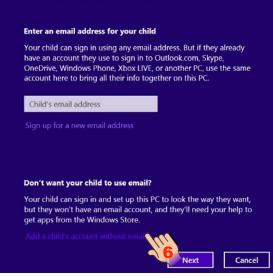




- Do not fill in an email in the field.
   Click or tap on Add a Child's Account.
- 6. Here you can enter an email address for you child or not. The following steps are for adding an account without an email address.
- 7. Enter your child's name and create a password for them. I suggest always setting up passwords even if this is only used at home. Make sure to add the password hint but do not make the password hint the same as the password. Click the Next link at the bottom.
- Your child's account is created.
   Now all you have to do is click
   Finished.
- 9. Now that you have your child's account all set up, it is time to set the Parental Controls. Windows 8.1 calls it, "Family Safety." You will now want to go back to the User Account Screen. You can get there by clicking the Start button Control Panel ➤ Set up Family Safety for any User. The steps are the same as Windows 7.













# Parental Controls for Windows 10

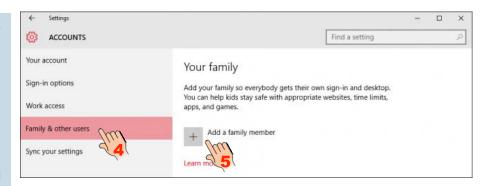
Microsoft has greatly improved parental controls and has included some monitoring features which will make our lives as parents a bit easier. If for no other reason, this is a good reason to upgrade to Windows 10.

You you haven't already, must first create your own Microsoft account at: https://account.microsoft.com/account

- 1. Go to the Microsoft account sign-up page and tap or click Create account.
- 2. In the User name box enter your existing email address, or tap or click Get a new email address to create an Outlook or Hotmail address.
- 3. Fill out the rest of the form, and then tap or click Create account.

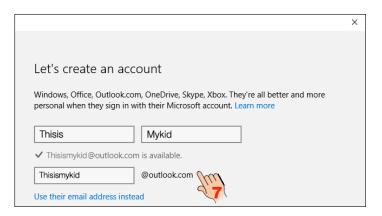
### Setting Up a Child's Account

- 4. In Windows 10, you will want to open up the Settings, then Accounts, and click on "Family & other users", then
- 5. Click "Add a family member".
- On the next screen, click "Add a child". It's a good idea that each member of your family, including children, have their own account.

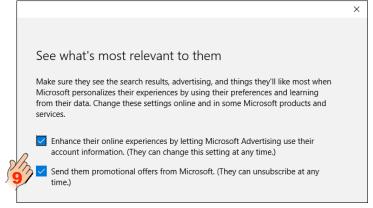




- 7. Next, you will fill in all the information needed to set up your child's account. If they do not have an email account, you can set up an outlook.com account for them.
- 8. Enter a telephone number to recover your child's password. This way if you're ever unable to access the account, such as if it is hacked or you forget the password, you can have a code sent to your phone that will let you reset it.
- On the next screen, you can check or uncheck these boxes, It is entirely up to you.
- Your child can now log into their account for the first time, and you can set up and configure their account settings using the Microsoft Family Safety tools online.







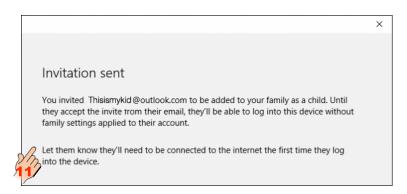


Alternatively, if you have already established an account for your child and you're simply adding it to your Windows 10 installation, you will need to make sure to confirm their account before any existing family settings can be applied to their account.

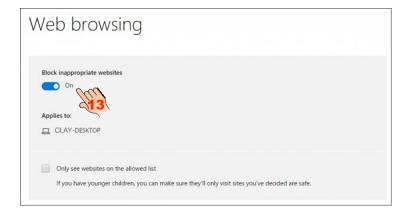
- 11. Until you do so, you will see that their account is still pending. They will be able to sign in and use the computer, but they won't have the protections you have established, so make sure to confirm their account using the email address you signed them up with.
- 12. With your child's account added, you're ready to head to the Family Safety website. Click "Manage family settings online" to open a browser and head there now.

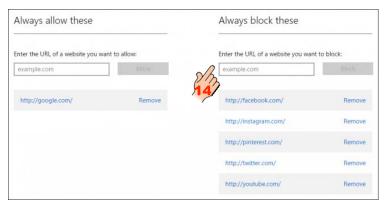
Once you've added your child's account, you can manage those family safety settings from the Family Safety website. The recent activity settings will collect your child's activity and email reports to you, both of which you can disable.

- 13. The first item you will want to consider is the "web browsing" category. You can "block inappropriate websites" and there is a check box to constrain your child's web browsing to only websites on the allowed list.
- 14. Here, you can explicitly allow and block websites. If you elected to "only see websites on the allowed list," then this will be where you will add websites to the "Always allow these" list.









- 15. The next category is to limit apps and games from three to twenty-year-olds, or not at all. Note, as you change the age, the ratings will change as well.
- You can also explicitly allow or block apps and games, just as you would with websites.
- 17. Finally, you can choose when your child uses the computer. You can decide how early and late they can use it, as well as how many hours per day. This means that even though your child may be able to use the computer throughout the entire day, you can still limit how many hours they're allowed to use it.

Microsoft has greatly simplified how parents can apply controls to their children's accounts so if you're new to all this, you should find it pretty easy to figure out. Having such controls in place should give you peace of mind to let your kids use the computer without too much adult supervision.

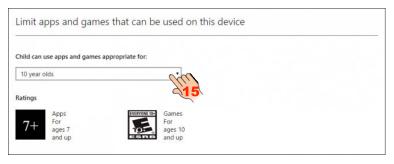
Keep in mind that if you add an existing account to your Windows installation, you won't be able to monitor it until you verify it via email. Until you do that, your child can log into the computer and it will not be monitored by Family Safety.

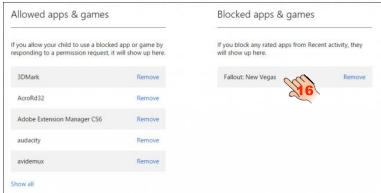
### Managing and Monitoring

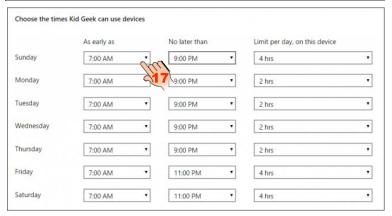
After you have your child's accounts set up, you can monitor some of their online activity and make adjustments to the parental control restrictions from your Microsoft account.

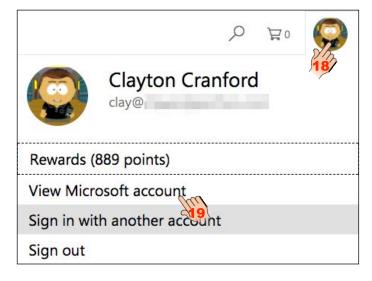
Go to Microsoft.com and log in to your account.

- 18. Click on your profile photo and then
- 19. Click on View account.





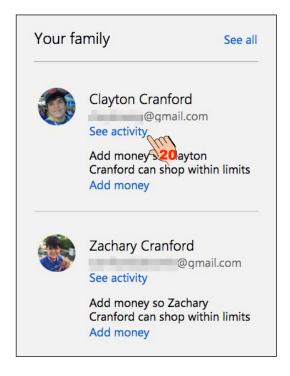


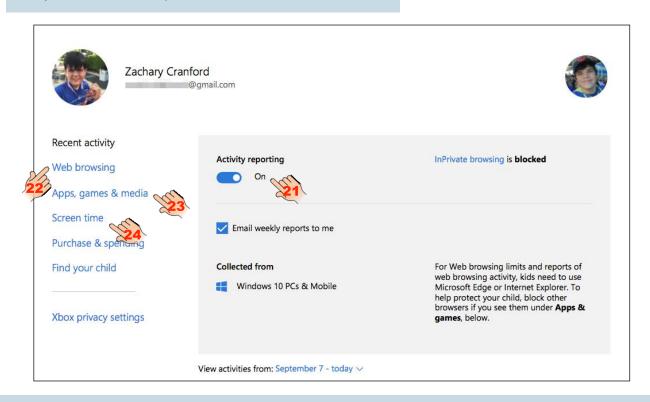


20. On the left column, you will see your account information and your Family accounts. Every child account created should be listed here. If you want to see your child's online activity or make changes to their restrictions, click on See activity.

Here, you can make changes to their parental control restrictions or view their online activity. For Web browsing limits and reports of web browsing activity, kids need to use Microsoft Edge or Internet Explorer. If you child is using Google's Chrome, their activity will not show up here. Most teens in schools today are using Google's Apps and Chrome in their classroom, so your information here may be limited.

- 21. Make sure Activity reporting is switched on and InPrivate browsing is Blocked.
- 22. Web browsing information is found here. Recent searches, blocked sites that your child attempted to access, and browsed sites are listed here.
- 23. Apps and games played are listed here. You also have the option to block them here as well.
- 24. Screen time is an issue that seems overwhelming for parents to police. Thankfully, you can see exactly how much time your child is on their computer. Additionally, you can create or adjust screen time limits here too.





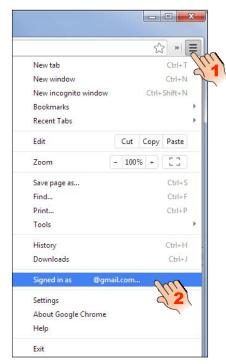






First, log In With Your Own Parent Account. You can only use and manage Supervised Users account if they're linked to a main parent account — that's your account.

- 1. Click the menu button
- 2. Look for the **Signed in as** option to verify that your account is logged in.
- 3. Uncheck guest browsing and restrict sign-in to the following users. This will prevent your child from using the guest account or logging in with another Google account to bypass the Supervised Browsing restrictions.
- Open Chrome's Settings screen from the menu and click the Add User button under Users. On a Chromebook, click the Add user option at the bottom-left corner of the login screen.

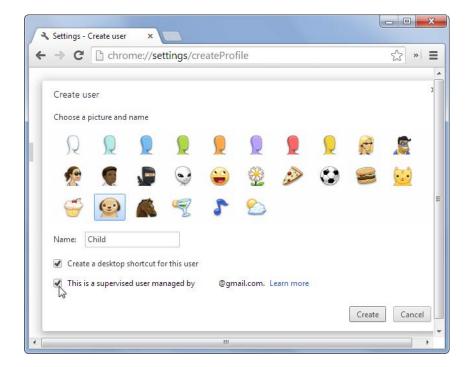






# Parental Controls for Chromebook Continued

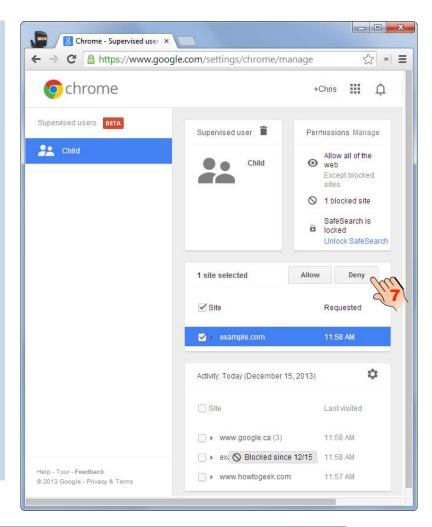
- 5. Create a new user account and select **This is a** supervised user managed by (your user account)
- 6. You will be prompted to create a separate password for your child. Their entire user account will be locked down. Just sign out of the Chromebook and have them sign in from the login screen.

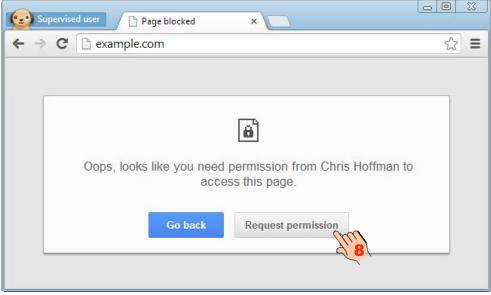




## Parental Controls for Chromebook Continued

- 7. To manage the account restrictions, you'll need to visit Google's management tool at www.chrome.com/manage. Sign in with the username and password you associated with your own parent account, not the one associated with the child account. After signing in, you can modify the permissions for all your Supervised Users. You can also view their browsing activity and allow or deny any requests they've made to unblock websites.
- 8. When a user accesses a blocked site, they'll see a "you need permission" screen. They'll be able to click the Request permission button and any permission requests will appear on the management page. You can access this page from anywhere, so you could approve access to websites even if you're not at home.







# Parental Controls for Mac OS



- 1. Click on the **Apple symbol** in the top left corner of your desktop screen.
- 2. Select **System Preferences** in the drop down menu.
- 3. Click on **Parent Controls** in the System Preferences window.
- Create a new user account or modify the current account that is logged in.





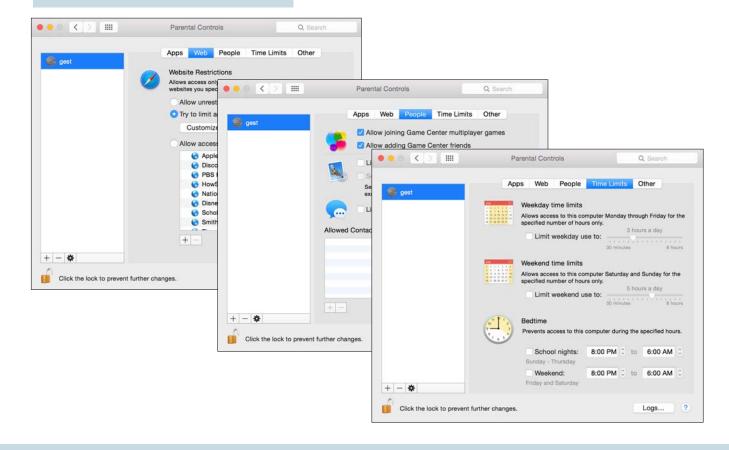


# Parental Controls for Mac OS Continued

#### Control Options

- Apps Restrict what applications are available to your child.
- Web Restrict web content or create a list of website which they can only visit.
- People Control the joining of multiplayer games through Game Center and whether they can add their own "friends" on Game Center. Limit mail and messages to a select group of contacts.
- Time Limits Set time limits.
- Other Disable the built-in web camera and disable the changing of the account's password.
- 6. Lock to prevent further changes.







# Parental Controls for iOS

(iPhone, iPad, & iPod)



- 1. Tap the **Settings** app.
- 2. Choose **General** for menu.
- 3. Scroll down to Restrictions. If you have never set up parent controls yet, it will show "off." Choose **Restrictions**.
- 4. Enable Restrictions.
- 5. Choose a passcode that only you know as the parent. Never share this with your child.









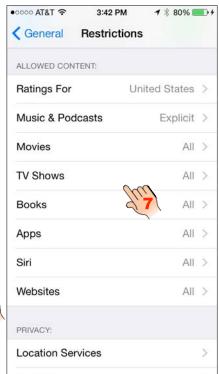


# Parental Controls for iOS (iPhone, iPad)

### Continued

- G. The first section of the Restrictions menu will allow you to turn off select applications, such as Safari browser or the Camera (Green means on, greyed out means off). In the second section, be sure to turn off App Installing, deleting, and In-App Purchases.
- 7. The third section filters content from various sources. Tap on any of these to the follow-on screen.
- 8. Check the ratings you want to allow. The blocked ratings will be listed in red.
- Scroll to the bottom of the menu to turn off Game Center's Multiplayer games and adding friends for children under 13 years old.













# Parental Controls for Android

Google has consolidated parental controls and monitoring for parents in one place: the Family Link app.

The Family Link app from Google helps you stay in the loop as your child explores on their Android device. With a Google Account, your child will be able to use Google's broad ecosystem of services for the first time. Here's how it works: First, your child will need a new device that runs Android Nougat (7.0) or higher. Then, download Family Link onto your device (Android or iPhone) and create a Google Account for them through the app. Finally, sign them into their new device, and you can then use Family Link to help you:

- Manage the apps your kid can use Approve or block the apps your kid wants to download from the Google Play store.
- Keep an eye on screen time See how much time your kid spends on their favorite apps with weekly or monthly activity reports, and set daily screen time limits.
- Set device bedtime Remotely lock your kid's device when it's time for bed, or time to take a break.

At the time of print, Family Link was still in beta, and to get enrolled you must request an invite to the Family Link early access program. After receiving an invite, download and try out the Family Link app. https://families.google.com/familylink/

## Create an account in the Family Link app

You need to be part of the Family Link early access program to create an account for a kid under 13 in the Family Link app.

It takes about 15 minutes to create your kid's Google Account.

- 1. Open the Family Link app.
  - . In the top right, tap Create . +
- 3. Follow the instructions on screen to create the account.
- 4. When you're done, a confirmation will show on the screen.

Create an account when you set up an Android device

Follow these steps to create a Google Account for your kid under 13 when you're setting up a device running Android 7 or up.

- Follow the instructions on screen to set up the device.
- When you're asked to sign in with your Google Account, tap More options Create new account.
- 3. Enter your kid's name, birthday, gender, email address, and password.
- 4. You'll see a "Link your account to a parent" screen. From here, follow the instructions to sign in with your own Google Account, provide parental consent, and pick your kid's settings.

#### Family Link to do things like:

- Change your kid's Google Account settings:
   Reset your kid's password, and manage certain
   Google Account settings, like access to websites
   on Google Chrome.
- Manage your kid's Android apps: Decide which apps your kid can download or purchase, block or allow apps, and change app permissions.

# Parental Controls for Android Continued

- Manage your kid's Android device screen time: Set a bedtime or daily screen limits, and see how much time your kids spend on certain Android apps.
- Check your kid's Android device location
- Restrict mature content on Google Play

# Restrict Inappropriate Websites on Chrome

When parental controls are turned on:

- Kids can't use incognito mode, or sign out of Chrome.
- Parents can manage the sites their kids can visit on Chrome, and some site permissions.
- By default, Chrome tries to block sexually explicit and violent sites.
- Chrome Sync is required for certain parental management features to work, so it can't be turned off completely. However, you can turn off certain kinds of data collection.
- Your kid's Google Activity controls might allow Google to use Chrome browsing history and activity from websites to personalize their experience across Google products and services. However, this information won't be used to personalize ads.

Manage your kid's activity on Chrome

Choose your kid's Chrome website restrictions

- 1. Open the Family Link app Family Link.
- 2. Select your kid.
- 3. On the "Settings" card, tap Manage Settings and then Filters on Chrome.
- 4. Choose the setting that's right for your family:
- Allow all sites: Your kid will be able to visit all sites, except the ones you block.
- Try to block mature sites: No filter is perfect, but this should help hide sexually explicit and violent sites
- Only allow certain sites: Your kid will only be able to visit the sites you allow.
- 5. Tap Manage sites to allow or block certain sites.

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

#### Block or allow certain websites

If you block a certain site, your kid can ask permission to visit it. You'll get a notification in the Family Link app where you can approve or deny their request.

Websites: If you block or allow specific website, like www.google.com, the permission won't apply to sites that begin or end differently, like www.google.co.uk or get.google.com/tips.

Domains: If you block or allow an entire domain, like google, the permission applies to sites that begin or end differently too, like google.com, and images.google.fr.

#### Block or allow a site

- 1. Open the Family Link app Family Link.
- 2. Select your kid.
- 3. On the "Settings" card, tap Manage Settings and then Filters on Chrome and then Manage sites and then Approved or Blocked.
- 4. In the bottom right corner, click Create Create.
- 5. Add a website or domain.
- 6. In the top left, click Close Close.

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

#### Change website permission settings

You can decide whether your kid can give permissions to websites they visit, including location, camera, and notifications.

- 1. Open the Family Link app Family Link.
- 2. Select your kid.
- 3. On the "Settings" card, tap Manage Settings and then Filters on Chrome and then Chrome dashboard.
- 4. Turn "Permissions for sites and apps" on or off.

When "Permissions for sites and apps" is off, kids shouldn't be able to give permissions to websites in the future. However, permissions they already granted will still be in place.

# Parental Controls for Android Continued

When you turn on parental controls, you can restrict what content can be downloaded or purchased from Google Play based on maturity level.

For family members 13 or older

How Google Play parental controls work

- Parental controls only apply to the Android device you added them on. To add parental controls on another device, repeat the steps below on the other devices.
- If you have multiple users on a device, you can set up different parental controls for each person.
- The person who sets up parental controls will create a PIN that needs to be entered to remove or change the parental controls.

#### Set up parental controls

- On the device you want parental controls on, open the Play Store app Google Play.
- 2. In the top left corner, tap Menu Menu and then Settings and then Parental controls.
- 3. Turn "Parental controls" On.
- Create a PIN. This prevents people who don't know the PIN from changing your parental control settings. If you're setting up parental controls on your kid's device, choose a PIN they don't already know.
- 5. Tap the type of content you want to filter.
- Choose how to filter or restrict access.

Once you set up parental controls, you can turn them on or off. When you turn them back on and create a new PIN, your old settings will come back. This helps you share a device with people who don't need parental controls.

For family members under 13

If you created a Google Account for your kid under 13, you can set up parental controls for them.

#### Set up parental controls

- 1. Open the Family Link app Family Link.
- 2. Select your kid.
- 3. On the "Settings" card, tap Manage Settings

and then Controls on Google Play.

- 4. Tap the type of content you want to filter.
- 5. Choose how to filter or restrict access.

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

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

#### Apps & Games

When you set up parental controls for apps and games, you can choose the highest content rating you want to allow for downloads or purchases.

If you try to install a game using the Play Games app, you'll be taken to the Play Store app where your parental controls settings may restrict access.

#### Movies

When you set up parental controls for movies, you can choose the highest rating you want to allow for rental, purchase, or playback.

#### TV

When you set up parental controls for TV shows, you can choose the highest rating you want to allow for purchase or playback.

#### **Books**

When you set up parental controls for books, you won't be able to read or purchase most sexually explicit books from the Play Store app and the Play Books app.

While setting up parental controls won't catch 100% of sexually explicit books in Google Play, it should help you avoid most adult content.

#### Music

When you set up parental controls for music, you won't be able to purchase music that's marked Explicit by content providers.

Parental controls for music only apply to the Play Store app. Parental controls don't change the music you see in the Play Music app, including purchased music, uploaded music, or subscription tracks.



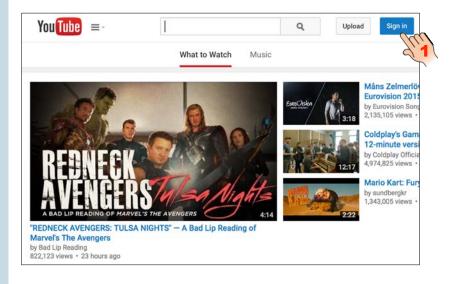


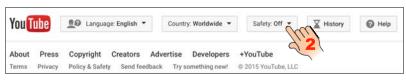


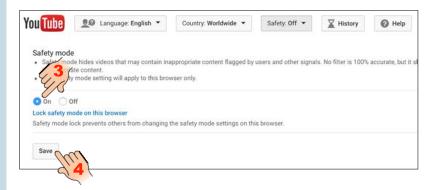
To filter out adult and inappropriate content on YouTube, "safe search" settings must be put on every browser and YouTube app, on computers and mobile devices. Launch a browser window and type www.youtube.com in the web address bar.

- Click the blue Sign In button in the top right corner of the screen and follow the prompts to sign in.
- Once YouTube loads, Scroll down to the bottom of the page and click the **Restricted Mode** button.
- 3. Click On
- 4. Click the **Save** button. To lock these changes so no one can change them without your password, click "Lock safety mode on this browser." You'll be prompted to enter your password. Once that information is entered, the feature is locked and can only be unlocked by entering your password again.

You'll know the parental controls are activated when you do a search. Stated at the top of the search results will be the phrase "Some results have been removed because Safety mode is enabled." You need to do this for any and all browsers on your computer that you think your child might use to access YouTube. The process is the same.



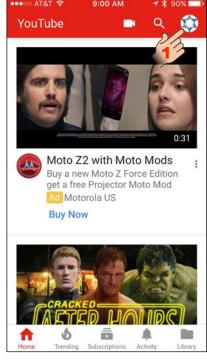


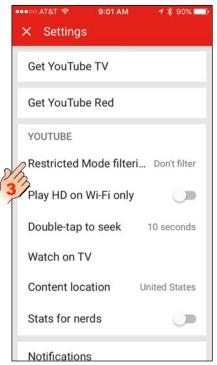


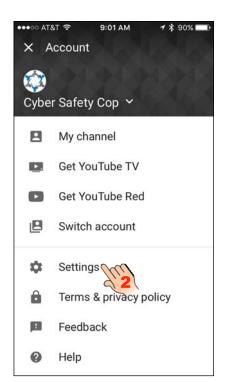


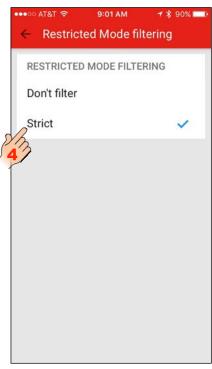
# YouTube Safe Search iOS App

- Open YouTube Mobile App. and tap your account image in the top right corner.
- 2. Tap **Settings**.
- 3. Select Restricted Mode Filtering.
- 4. Select Strict.





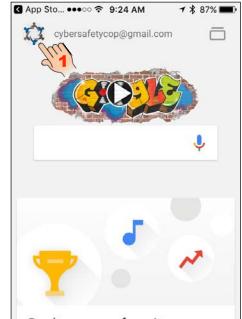


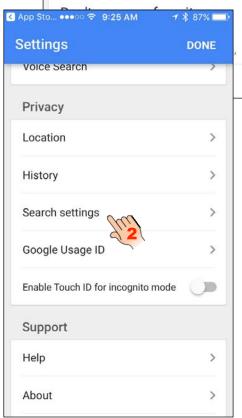




# Google Safe Search iOS app

- Open Google Mobile App. and tap your account image in the top left corner.
- 2. Scroll down and tap **Search Settings**.
- 3. Select Filter explicit results.







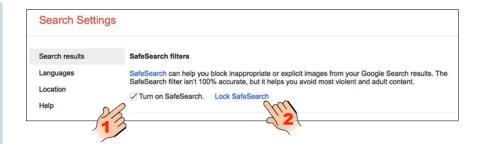


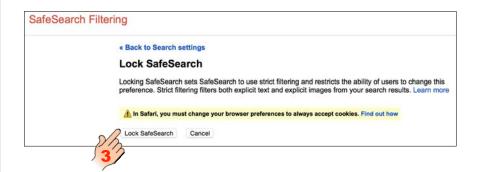




Google Safe Search settings filter out adult content showing up in search results. These settings must be applied to every browser on every computer.

- Enable all third-party cookies in your browser's settings/ preference panel.
- 2. Open the browser and navigate to google.com and sign in to your Google account. Then navigate to http://www.google.com/preferences. Check Filter explicit results.
- Select Lock SafeSearch and sign back into Google.
- 4. You will see colored balls and "SafeSearch is locked" in the top right corner of the browser which will indicate that Safe Search is on. Reverse the steps to unlock.









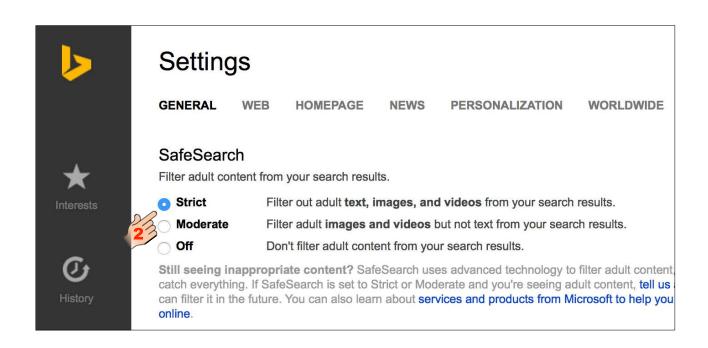
# Bing Safe Search

**Desktop Browsers** 



Bing is Microsoft's default search engine in Internet Explorer. Enable Safe Search to filter out adult content from search results.

- 1. Navigate to:
  - http://www.bing.com/account/general, Bing offers two levels of filtering.
- Strict filters adult text, images, and videos from results, while Moderate applies the filter to only images and video (text remains unfiltered.)





# Yahoo Safe Search

Desktop, iOS, and Android

# Access SafeSearch settings

You can quickly access SafeSearch settings on your desktop and mobile devices.

### Desktop

- 1. Sign in to Yahoo.
- 2. In the search box, enter a search and click Search.
- 3. From the search results, mouse over the Settings icon Settings icon.
- 4. Click Preferences.

#### Android

- 1. Go to https://search.yahoo.com/.
- 2. Tap Settings.

#### iOS iPhone

- 1. Go to https://search.yahoo.com/.
- 2. Go to the bottom and tap Settings.

#### iPad

- 1. Go to https://search.yahoo.com/.
- 2. Tap Settings.
- 3. Scroll down and tap Sign in.
- 4. Change or lock SafeSearch

You can change the filter strength of SafeSearch, and lock in your choice for each browser on your computer or mobile device.

#### Change SafeSearch strength

- Select an option from the SafeSearch dropdown menu:
- Strict no adult content
- · Moderate no images or video



- Off do not filter results
- 2. When you're done choosing, click or tap Save.

#### Unable to turn off SafeSearch?

- You may be signed in to a Yahoo Account that's registered as an under-18 account.
- You may need to contact your Internet Service Provider (ISP) for further details.

#### Set a SafeSearch Lock

Using an iPhone? - SafeSearch can't be locked on an iPhone, right now.

You can lock the SafeSearch setting for each browser on your computer or mobile device. Once you've locked SafeSearch for a browser, it's locked in that browser on the computer or mobile device you were using, for users who have:

- Not signed in to a Yahoo account.
- Signed in to an account that's under 18.

#### Lock SafeSearch

- Access SafeSearch settings using the steps above.
- 2. Select an option from the SafeSearch dropdown menu.
- 3. Click or tap Lock.
- 4. Click Save.
- 5. Sign out of your Yahoo account.

#### Unlock SafeSearch

The lock can be disabled from a Yahoo account that is registered as over 18. An extra verification step must be passed to confirm that the user disabling the lock is over 18 years of age.



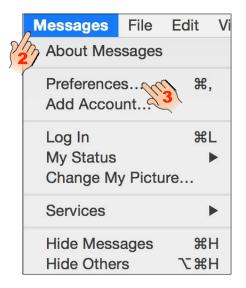


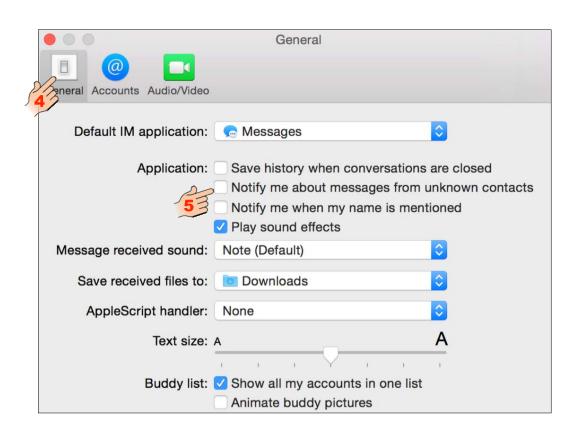


# **Desktop Settings**

- 1. Open the **iMessage** App.
- 2. Click on **Messages** in the app's tool bar to drop down menu.
- Select Preferences.
- 4. Select General.
- 5. Uncheck Notify me about messages from unknown contacts.







# Apple iMessage Privacy Continued

# iOS Settings

- Open the Settings App.
- 2. Scroll down and select **Messages** from the menu.
- 3. Turn on (green) Filter Unknown Senders.

# To Block a Contact

- Open the Settings App. Scroll down and select Messages from the menu. Select Blocked.
- Add contact from your contact list to be blocked from calling or messaging your child.















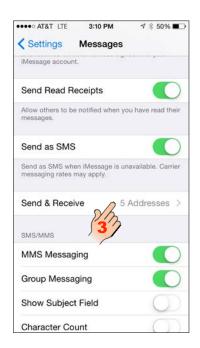


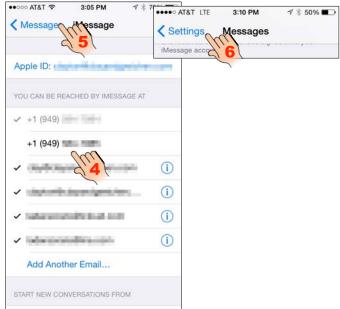
If your child wants to use text messaging, iMessage is by far the safest choice. Do not let them use instant message apps like Kik or TextNow. You have two choices. One, you can keep you child under your iCloud account or you can create a unique iCloud account for them. I recommend keeping your child on your iCloud account so their phone number appears in your Messages menu. By following the directions below, you will be cc'd on all your child's messages.

- Open the Settings App.
- 2. Scroll down and select **Messages** from the menu.
- 3. Select Send & Receive.
- 4. Click on your child's phone number. A check mark will appear next to it.
- 5. Go back to Settings by selecting **Messages.**
- 6. Then **Settings**.









# Apple iMessage Monitoring Continued

Select General.
 Select Restrictions and enter your parental passcode.
 Select Accounts.
 Select Don't Allow Changes.











# Instagram Privacy Settings & Reporting Abuse

Instagram is currently the most popular image/messaging social network among teens. It has straight forward privacy and abuse reporting features.

# Setting Private Account

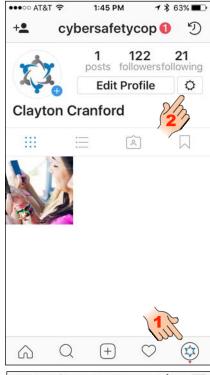
- 1. Open the Instagram App. Select the Profile icon.
- 2. Select Settings 💢 icon.
- Turn on (blue) Private Account.

# Reporting Abuse

 Navigate to the account, image, or comment that you want to report as spam or abusive.

Select ••• to open the Reporting sub-menu.

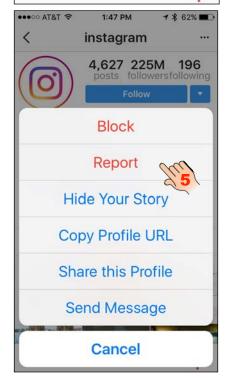
Follow the sub-menu prompts to the correct category













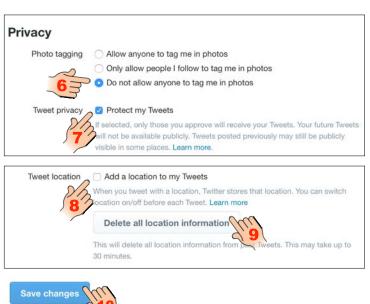
# Twitter Privacy & Security Settings Desktop



The settings below are for the strictest privacy settings. 1. Log into Twitter and click on your profile picture. 2. Select **Settings** from drop down menu. 3. Select **Security & Privacy**. 4. Choose **Send login verification requests to** [your mobile phone]

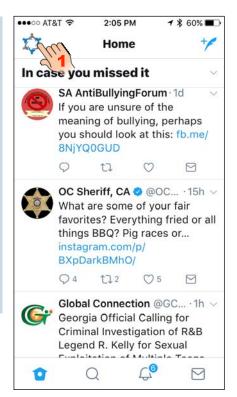


- 5. Check Require Personal information to reset my password.
- 6. Select **Do not allow anyone** to tag me in photos.
- 7. Check Protect my Tweets.
- 8. Uncheck Add a location to my Tweets.
- 9. Click **Delete all location** information
- 10. Save Changes

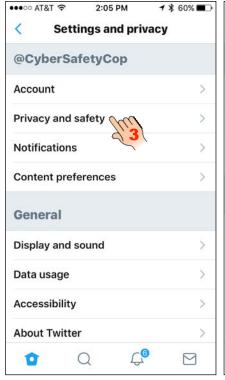


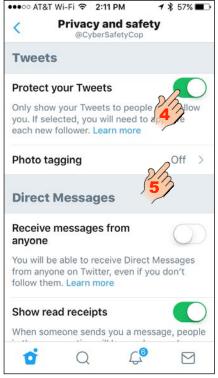
# Twitter Privacy & Security Settings iOS

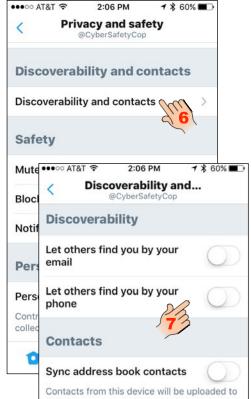
- Open Twitter on your iOS device. Click on your profile image.
- Select Settings and privacy.
- 3. Select Privacy and safety.
- 4. Turn on **Protect your Tweets**.
- 5. Turn Photo tagging Off.
- 6. Scroll down and select **Discoverability and contacts**.
- 7. Turn off all discoverability options.















# Facebook Privacy Settings

Do you think your child's Facebook page is private and secure? Can only approved friends see your child's personal information like the city they live in, birthday, or mobile phone number?

Use the steps below to test what your personal, or your child's, Facebook account looks like to a stranger.

- 1. Go to your profile and click ••• in the bottom right corner of the cover photo.
- 2. Click View As.

A truly private profile should display only the account name, profile image, and cover photo. If you see posts, pictures, or personal information you need to follow the directions on the proceeding pages.





# Facebook Privacy Settings

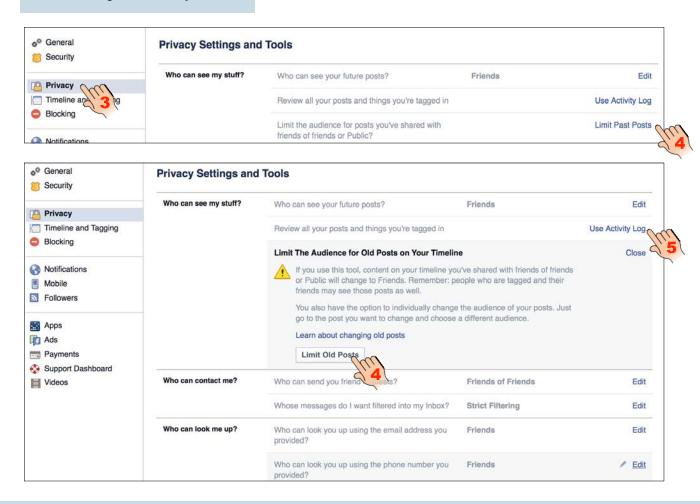
# **Desktop Browser**

- Click the downward arrow in the right bottom corner of your cover photo.
- 2. Select Settings.
- 3. Select Privacy
- Select Limit Past Posts so your old post can only be seen by you and your friends.

Select Confirm.

 You can Use Activity Log to view all your posts, comments and likes. You can manage your old posts here, deleting them one-by-one.

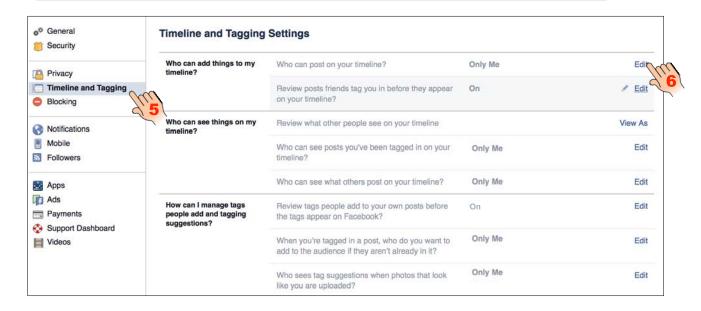




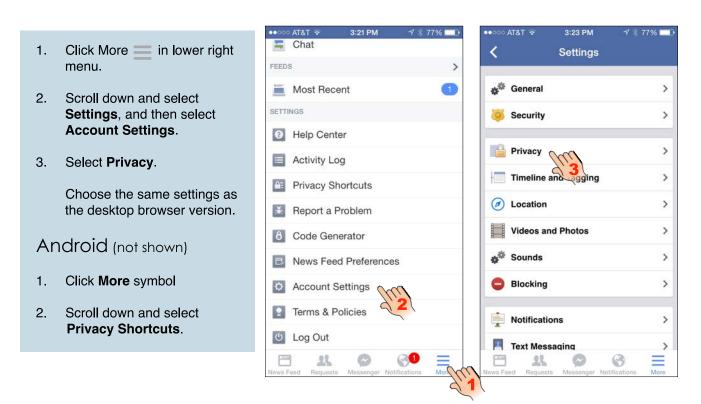
# Facebook Privacy Settings

Desktop Browser Continued

5. In "Settings," select **Timeline and Tagging**. 6. Set to **Only Me** for strictest privacy setting. The settings below are the set to the most private options.



# Facebook Privacy Settings ios Mobile App



# Facebook Blocking Abuse

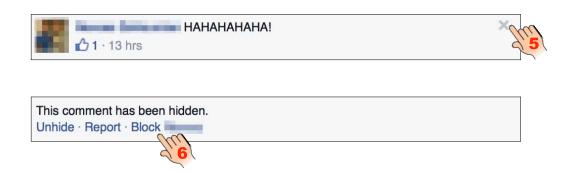
# Desktop Browser

1-2. Select **Settings** from drop down menu, 3. Select **Blocking**, 4. Type in the name or email of the person you want to block.



To block or report a comment,

- 5. Click on the **X** in the top right corner of the comment message box.
- 6. Select either **Report** or **Block**.



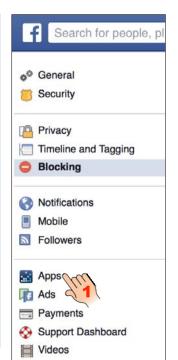
# Facebook App Sharing Settings

# Desktop Browser

 Apps can share information and preferences. Their connections remain even after you delete the parent app off your device.

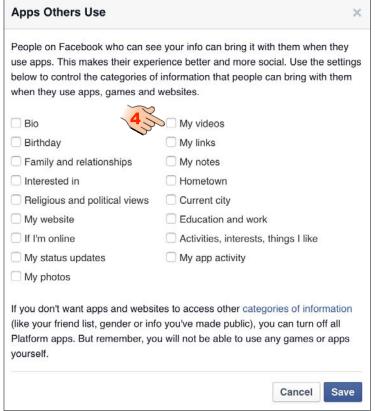
From the settings menu, select **Apps**.

- Delete apps that you are no longer using by clicking on the X.
- 3. Scroll down and select **Edit Apps Others Use**.
- 4. Uncheck information you don't want to share with other apps.



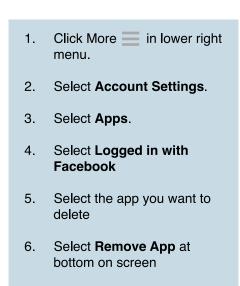


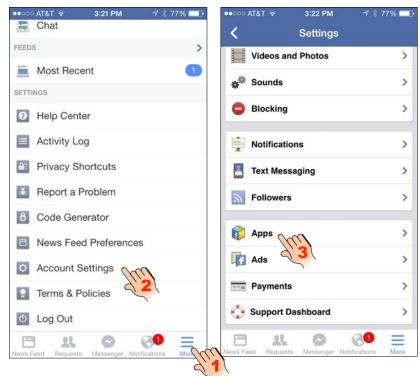


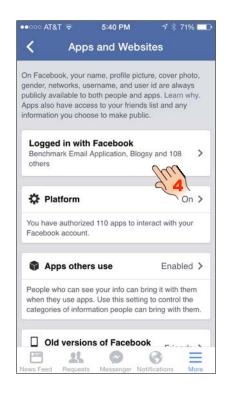


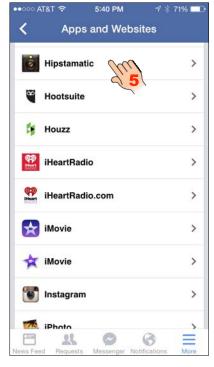
# Facebook App Sharing Settings

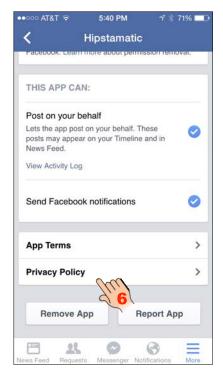
# iOS Mobile App









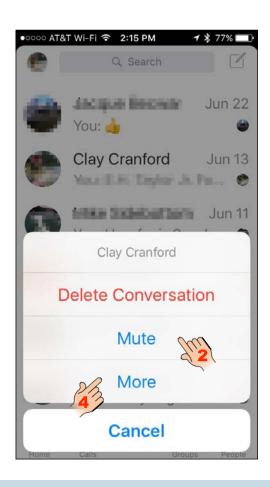


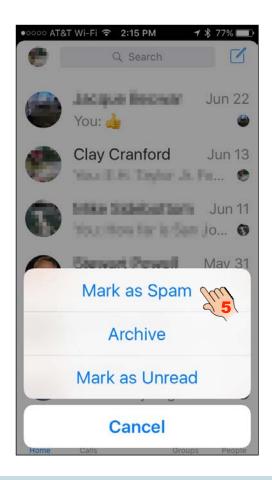






- Select Recent messages.
- 2. Press and hold on a message to reveal the submenu. To stop receiving messages from this contact, select **Mute**.
- 3. Select how long you want the contact muted.
- 4. To block report the sender as spam, select **More**.
- 5. Select Mark as Spam.





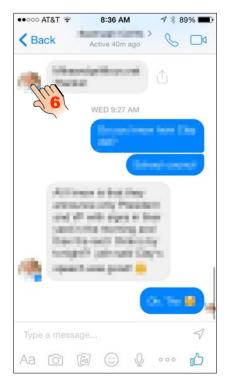
# Facebook Messenger Blocking

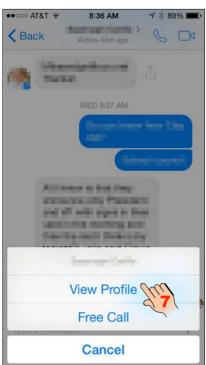
# Continued

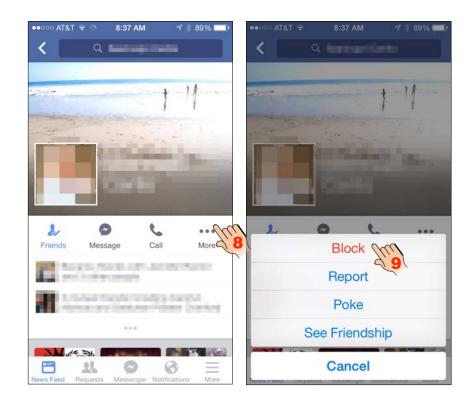
- 6. To block the contact from both Facebook and Facebook Messenger, tap the profile picture from the message window.
- 7. Select View Profile.
- 8. Select More.
- 9. Select Block.

#### Android OS (not shown)

- Go to Settings and turn off Synced Contacts, and Location.
- Select **Privacy** in the small print links at the bottom of the settings page.











# Cyber Safety Training

You can bring Cyber Safety Cop training to your school, workplace, law enforcement agency, or organization. Total Safety Solutions offers several training opportunities that can be tailored to fit your organization's needs.

# Cyber Safety Seminar for Adults

Based on Clay Cranford's acclaimed book, Parenting in the Digital World, this 2-hour 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.

The class first explains the current technology and applications teens are using to access the Internet and social media networks. 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.

Participants will receive an Internet Safety Contract and the Cyber Safety Checklist. This class is for adults only. Children are not permitted.

# Cyber Safety Assembly for Students

Cyber Safety for Students is a 40 minute interactive presentation for students 5th to 12th grade. It can be taught in a classroom or in a gymnasium to hundreds of students. Cyber Safety for Students gives students the information they need to make good decisions in their online lives. Additionally, the Cyber Safety class will show them common vulnerabilities to their safety and how they 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 and sexting can have on their lives. Topics include:

- Don't allow strangers in your network
- Don't share inappropriate images
- Create a positive online reputation
- Consequences of mean, rude, or threatening messages

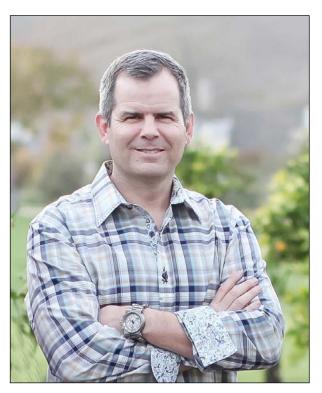
Cyber Safety for Students complements Cyber Safety for Parents. The concepts covered in the Student class are explained in the parent class, allowing parents to follow up with their children and reinforce what they learned at school.

Contact the Cyber Safety Cop team to learn more at: www.CyberSafetyCop.com



# 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 was also a member of Orange County, California's school threat assessment team. He has investigated threats, weapon possession, in nearly 200 schools. 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 with two boys 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 ASTEP-BY-STEP GUIDE TO INTERNET SAFETY SECOND EDITION

"Parenting in the Digital World is brilliantly organized, easy to follow, and offers screen shots and step-by-step instructions on how to manage the privacy settings on different operating systems and applications. Knowledge is power and I am delighted to recommend this empowering book! Together, we can stop crimes against children. Be Brave."

-Erin Runnion, Founder of The Joyful Child Foundation

"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 second 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, threats and consequences, how to protect yourself from being hacked, and how to create a culture of safety and accountability in your home.

