TECHNOLOGY & YOUR KIDS

BY MARK TIMM
Like most moms and dads, I started the journey of parenthood with a fairly high level of confidence in my ability to successfully raise a child. I had read all the how-to books so by the time the first baby arrived, I felt well-armed with an arsenal of practical parenting advice. Same for the second, and third...

And then those babies became pre-teens and teens, and the game changed.

Suddenly, my wife and I found ourselves absolutely overwhelmed at our children’s ability to access information via technology that didn’t exists a few years ago. Whereas in the toddler years, we fairly easily managed our kids’ use of technology and limited it to some children’s programming on television, Disney movies, and maybe the occasional “educational game” on the computer, suddenly we found ourselves faced with tech-savvy kiddos who often help us know how to navigate our own devices!

Among our friends, we’ve heard similar concerns:

- “I have no idea what to do.”
- “It is not what I grew up with.”
- “I don’t understand it.”
- “I have no idea what they are doing, and it scares me!”
- “It is a part of their life in a way I will never be able to appreciate or comprehend!”

As parents, we all know that we have to step up and actively manage this technology situation, but the sheer magnitude of the task can lead to inertia. According to a recent article in The Washington Post,

87 percent of parents say they have rules for their children’s technology use, though the kinds of rules they set vary widely. For example, 19 percent of parents limit their kids to five hours of tech use or less per week. A little more than one-third, 35 percent, set no limits at all.

Meanwhile, only 36 percent use parental controls to limit their kids’ tech use—with many
saying they don’t see the need to because they trust their children’s judgment and other household rules to keep things in hand. Three in four parents said they have taken away or limited access to the Web as a punishment for bad grades, breaking rules or other bad behaviors.

But there was also a slight dip in the number of parents who said they feel they have a handle on what their kids are up to online. And 55 percent said that they let a child under the age of 12 open a social networking account—something that is only allowed for kids 13 and up.”

Chances are if you’re reading this, you don’t need convincing that technology is a parenting issue that must be faced head-on. You wholeheartedly agree, but you’re looking for some tips and strategies for doing just that—managing technology usage and access in your household.

**An important thought to keep in mind, though, is that the problem is not just the technology.**

In his *Understanding Teenagers* blog, Chris Hudson reminds us,

> "If you believe that the problem with what teenagers do online is a technological one then you are missing a vital truth. Technology does not make teenagers do things. Teenagers are responsible for their own behavior.

Equipping teenagers to manage their online worlds and digital technology responsibly is a behavioral issue not a technology issue. Once parents stop focusing on technology as the problem and the negative bias that accompanies it, they realize the requirement of managing technology related behavioral issues with teenagers is the same as for any other parenting challenge.

There is no new special code to unlock or parenting mountain to conquer. Instead, digital parenting is about the same old topics parenting has always been about: instilling values, teaching skills, establishing boundaries, nurturing confidence, building trust, and fostering responsibility.”

To that end, what follows are some practical tips and strategies that you can start implementing today so that you will gain the confidence you need to navigate parenting in the digital age.
6 Ways to Set Technology Boundaries with Your Children

1. Have discussions about when, where, and how often it is appropriate for your kids to use technology, as well as what they can and can’t do online.

2. Have clear times when phones and tablets need to be turned off, such as meal times, during family meetings, movie night, game night, etc.

3. Set limits on the amount of game time allowed each day, and come up with sensible expectations for how much time is spent socializing online.

4. Keep all electronics out of kids’ bedrooms, including televisions. Instead require devices be used in common family areas.

5. Charge all devices in one central location at night—maybe the kitchen or living room, or even Mom and Dad’s bedroom.

6. Set the example for your kids by adhering to the same technology rules of etiquette.
From the moment my first child came into the world, my primary desire was to keep him safe. We go to great lengths to baby-proof our homes, don’t we? Safety latches, outlet covers, doorknob covers and table corner pads, and so much more. We teach stranger danger from an early age (as we should), and we rarely let our children out of our sight in a public place, even at the neighborhood playground.

Yet many parents are unaware of the real dangers that a child can stumble upon in the virtual world simply by pressing one button on a smartphone or laptop: child predators, cyberbullying, pornography, obscene language, and damaged reputations to name a few.

One way to monitor your child’s online safety is to limit all online access to a public area where the screen can be seen by anyone in the room. This works well for family desktops and laptops, but gets trickier with the smart phones and other handheld devices.

Some Internet sites provide their own protective features. For example, Google offers a Safe Search feature that can be activated to restrict search results shown to children, and YouTube safety mode gives users the opportunity to block mature content.

FIVE WAYS TO GUARD AGAINST MALICIOUS INTERNET CONTENT OR PREDATORS

An Internet filter is “hardware or software that restricts the information that is delivered over the Internet. Filters can greatly reduce the flow of harmful content onto your computer.

Filters can be installed on the servers of an Internet Service Provider or proxy service, as part of a local area network, or on individual computers. They can block access to websites, e-mail, chat, or other Internet-based communications based on category, site, or content.”

But be aware, installing a filter sometimes provides a false sense of security. “Most teenagers can get around just about any filter if they really want to, and parents need to know how this is done so they can watch for the warning signs. Also, be sure to use the tools that the filter provides, such as usage reports, blocked site reports, etc. A filter is not a silver bullet, and it is not a set-it-and-forget-it solution.”
FIVE DIFFERENT TYPES OF INTERNET FILTERS INCLUDE:

1. SOFTWARE

This is the most common filter, and it comes in the form of an application that is downloaded from the Internet or purchased in a store, then installed on your computer. The filter interjects itself into the communication chain between the applications on that computer and the Internet so it can watch the communication, and perform its guard duty. Software filters are usually the most robust, and offer the greatest level of protection—not only from pornography, but from other dangers as well (such as online predators, online gaming, etc.). K9 Web Protection and Qustodio are examples.

This option is like putting a guard at your front door. A software filter looks at data as it arrives on your machine. It is important to note that because the filter is actually installed on your computer, the bad content will exist on your computer, but the filter intercepts it before it displays on the screen.7

2. HARDWARE

When you have a broadband Internet connection, or an always-on connection, there is a physical device that you must use to connect your computer to the Internet. This may be a cable modem or a DSL router; it all depends on what type of broadband connection you have purchased. Some of these routers, or modems, have built-in software that filters the Internet. This is an example of a hardware filter—the hardware device that brings the Internet into your home can be configured so that it will filter the content before it arrives on your computer. You do not need to install anything on your computer; the mere fact that your computer uses this device to access the Internet ensures that the content is filtered. Hardware filters are usually simplistic and would only prevent access to inappropriate content.

This option is similar to the guard standing at your mailbox, intercepting the mail directly from the mailman before it is placed in your mailbox. The bad content is intercepted before it ever arrives on your computer.8

3. DNS

Another option is to use a DNS service such as OpenDNS to provide filtering. This provides a free option with many of the benefits of having a hardware solution, without having to purchase additional hardware because it will probably work with your existing home networking hardware.
This option has the advantage of filtering all of the devices in the home; including the computers, cell phones, TVs, game consoles, etc. Any device that would connect to your router, either by wire or wireless. Cell phones connected to the Internet via a cell tower will not be filtered.9

4. INTERNET PROXY

Some Internet Service Providers (ISPs) will offer filtering as part of their service. If they don’t, you could sign up with a service on the Internet, called a “proxy,” that will filter your content on the Internet before sending it to your home. Since this works on the Internet, there is nothing to install on your computer. If this service is offered by your ISP, then there is usually nothing to configure—you simply turn this service on with your ISP, and it filters all content. If you are using a proxy service, then you must configure your individual computer to use the proxy filter. It doesn’t necessarily install anything on your computer, but you do need to ensure that the computer is configured to use that proxy. Like hardware filters, Internet proxy filters are usually simplistic, and would not have the robust features of a software filter.

Continuing our analogy of a guard watching our mail, this would be comparable to our guard standing at the post office and inspecting each piece of mail before it is loaded onto the mail truck for delivery.10

5. VPN - VIRTUAL PRIVATE NETWORK

A VPN solution is becoming more popular today as more and more devices travel outside the home. Tablets and smartphones are making it increasingly difficult to filter the devices children use to connect to the internet. A software filter on a computer does not protect these smart devices. A hardware filter (like on a router) can protect these devices if they are connected to the WiFi home network, but not when 3G/4G mobile network is turned on. A DNS or proxy filter is hard to configure on a smart device, easy to bypass, and often doesn’t filter network traffic from apps. There are apps which attempt to protect a smart device, but they often require using a custom internet browser and do not protect other apps. A VPN filter is really the best solution for smart devices today because it protects all internet traffic (even from apps installed on the smart device). A VPN filter can also be used on a home router or directly on a computer. Some examples of VPN-based filters include NetAngel, Disney Circle Go, and PageClean.11
Apps and Social Media

In July 2014, the following statistics were released by Adjust, a mobile attribution and analytics company:

“Currently, there are 1,252,777 apps available in the (Apple) App Store, and as many as 60 thousand apps are added per month—and this rate is itself growing. In 2013, 453,902 new apps were released in the Apple App Store, exceeding Adjust’s prediction of over 435,100 new apps by 4 percent.”

Certainly great numbers of these millions of apps are harmless, and in fact likely are helpful in some way. But the apps that can be dangerous for children and teens are out there—lots of them—and it’s all but impossible for parents to stay on top of which ones are which.

Sexting, cyberbullying, hook-up apps—they’re all out there. And while your child may insist that she uses social media in only appropriate ways, can you trust that everyone she is connected with will do the same?

More than 200 eighth graders from across the country allowed their social media feeds to be studied by child development experts who partnered with CNN in the first large-scale study to analyze what kids actually say to each other on social media and why it matters so deeply to them.

“I think they’re addicted to the peer connection and affirmation they’re able to get via social media,” said child clinical psychologist Marion Underwood, the study’s co-author. “To know what each other are doing, where they stand, to know how many people like what they posted, to know how many people followed them today and unfollowed them ... that I think is highly addictive.”

The more teens look at social media, the study found, the more distressed they can become. The heaviest social media users admitted to checking their social media feeds more than 100 times a day, sometimes even during school hours.

So, let’s do the math. With millions of apps out there, and more being added daily, plus our kids’ compulsive, almost addictive, need to check social media a hundred times a day or more, the opportunity for exposure to undesirable content is all but impossible to avoid without intentional diligence on the part of parents.

The same CNN study found that despite the fact that 94% of parents underestimated some of the activity their children were participating in on social media, “Parent monitoring effectively erased the negative effects of online conflicts.” Parents that tried to keep a close eye on their child’s social media accounts had a profound effect on their child’s psychological well-being.
8 PRACTICAL TIPS FOR PARENTS TO BE PROACTIVE WITH SOCIAL MEDIA AND APPS

In addition to your general boundaries around Internet usage, create some rules specific to social media. These should include:

1. Keep personal information private. Make sure your child knows to never share his or her address, school name, sports practice schedule, etc. Many parents do not allow their children to use their full name on their social media profiles at all.

2. For each platform your child is on, know the password and access information. (Keeping a password journal is a good idea).

3. It’s important for you to be on the same platforms as your child, and require that he or she accepts you as a friend/follower on each one.

4. Be sure that you know, at least marginally, everyone your child is connected with on social media. Make sure no “friend requests” from strangers are ever accepted, even if there are mutual friends.

5. Use both the device security settings and the privacy settings in each application.

6. Post photos and words carefully, knowing they are potentially there forever: colleges and employers are increasingly using Internet searches to scan applicants’ social media pages. (One good rule of thumb: don’t post anything you wouldn’t want your pastor to see!)

7. To discourage kids’ tendency to be obsessed with their numbers of followers and likes, consider prohibiting apps that track these things (and there are hundreds of them available).

8. Check your child’s devices periodically and be sure you know what each app is for. Some apps to be aware of as potentially dangerous include the anonymous sharing apps Yik Yak, Whisper, Nearby, Secret, PostSecret, Kik, and Ask.fm. Two apps that are frequently used for “sexting” photos include WhatsApp and Snapchat. And absolutely ban “hook-up” apps such as Tinder, Blendr, Grindr, Skout, Down, and Pure.
4 Ways to “Trust but Verify”

We trust our kids, but they’re kids. They will make mistakes. They will find themselves in situations that they know they shouldn’t be in. And they have friends who won’t always meet our expectations.

There are some tools available to help parents monitor Internet and texting activity, and even a child’s location. If you fall into the “trust but verify” camp, here are some options to consider:

1. **WebWatcher Monitoring**: PC Magazine’s Editors’ Choice, records absolutely all activity on the child’s PC, Mac, iPhone, or Android. Parents receive real-time email notification when “alert words” appear. There are filtering options and time limit options available.

2. **MamaBear**: In addition to social media and text monitoring, plus location sharing, this app has a unique feature of notifying parents when and where your child is driving or riding faster than a speed you set.

3. **OurPact**: Allows parents to set limits on how much time children spend on mobile devices by creating schedules or blocking all internet and app use at a moment’s notice. Also has an “allowance” feature.

4. **TeenSafe**: Monitors texts (including deleted texts), views calls, sees phone location, shows web searches, and can view activity on Instagram, WhatsApp, and Kik.

We, as parents, are not the digital natives that our children are. Parenting in the technology age is evolving not by the day, not by the hour, but by the minute and second. It is incumbent upon us to do our due diligence and stay on top of developing trends—especially in social media—so that we can protect our children just as effectively from the potential dangers of the virtual world as we do from physical danger.
In my family, we have implemented use of contracts with our kids to help them take responsibility for their choices. We go over terms in advance, including discipline or consequences. When everything is clearly written down and agreed upon in advance, it takes the heartache out of the implementation of consequences.

There are many examples to be found with a simple internet search, but if you prefer to create your own, consider including some of the following language:

1. My use of technology is a privilege, not a right.
2. My technology will be placed in a common area for charging by (time) on weeknights and (time) on weekends.
3. My parents will have my passwords to all of my devices, as well as all apps on the devices. (I recommend keeping a password logbook!)
4. I will not use profanity or any inappropriate language as defined by my parents.
5. I will not send, share, or otherwise transmit pictures of myself or anyone else which would be considered inappropriate and/or embarrassing.
6. I understand that my parents can and will monitor all use of technology in the house and can access my accounts and devices at any time.
7. I will observe internet safety rules, which include not communicating with anyone I do not know and not posting any of my personal information. I will not lie about my age to access apps or websites.
8. I will check with my parents before downloading any software or apps.
Increasing loneliness and depression. While it may seem that losing yourself online will temporarily make feelings such as loneliness, depression, and boredom evaporate into thin air, it can actually make you feel even worse. A 2014 study found a correlation between high social media usage and depression and anxiety. Users, especially teens, tend to compare themselves unfavorably with their peers on social media, promoting feelings of loneliness and depression.

Fueling anxiety. One researcher found that the mere presence of a phone or other device nearby tends to make people more anxious and perform poorly on given tasks. The heavier the user, the greater the anxiety experienced.

Increasing stress. Have you heard the term FOMO? It means Fear Of Missing Out. Teens feel the pressure to always be connected, never out of touch from their friends. This need to continually check and respond to texts and other social media messages can contribute to higher stress levels and inability to focus on tasks such as school work.

Exacerbating attention deficit disorders. The constant stream of messages and information from an electronic device can overwhelm the brain and make it impossible to focus attention on any one thing for more than a few minutes without feeling compelled to move on to something else.

Diminishing your ability to concentrate and think deeply or creatively. The persistent buzz, ping or beep of your device can distract you from important tasks, slow your work, and interrupt those quiet moments that are so crucial to creativity and problem solving. Instead of ever being alone with our thoughts, we’re now always online and connected.

Is My Child Addicted?

Smartphones, tablets, or the Internet can be addictive because their use, just like the use of drugs and alcohol, can trigger the release of the brain chemical dopamine and alter mood. And just like using drugs and alcohol, you can rapidly build up tolerance so that it takes more and more time in front of these screens to derive the same pleasurable reward.16

Compulsive use of electronic devices can interfere with your child’s daily life, school or work, and relationships. When kids spend more time on social media or playing games than interacting with real people, or they can’t stop themselves from repeatedly checking texts and social media apps, it is time to question whether things have gone too far.

7 EFFECTS OF TECHNOLOGY ADDICTION ON KIDS

1. Increasing loneliness and depression. While it may seem that losing yourself online will temporarily make feelings such as loneliness, depression, and boredom evaporate into thin air, it can actually make you feel even worse. A 2014 study found a correlation between high social media usage and depression and anxiety. Users, especially teens, tend to compare themselves unfavorably with their peers on social media, promoting feelings of loneliness and depression.

2. Fueling anxiety. One researcher found that the mere presence of a phone or other device nearby tends to make people more anxious and perform poorly on given tasks. The heavier the user, the greater the anxiety experienced.

3. Increasing stress. Have you heard the term FOMO? It means Fear Of Missing Out. Teens feel the pressure to always be connected, never out of touch from their friends. This need to continually check and respond to texts and other social media messages can contribute to higher stress levels and inability to focus on tasks such as school work.

4. Exacerbating attention deficit disorders. The constant stream of messages and information from an electronic device can overwhelm the brain and make it impossible to focus attention on any one thing for more than a few minutes without feeling compelled to move on to something else.

5. Diminishing your ability to concentrate and think deeply or creatively. The persistent buzz, ping or beep of your device can distract you from important tasks, slow your work, and interrupt those quiet moments that are so crucial to creativity and problem solving. Instead of ever being alone with our thoughts, we’re now always online and connected.
Disturbing your sleep. Excessive technology use can disrupt your sleep, which can have a serious impact on your overall mental health. It can impact your memory, affect your ability to think clearly, and reduce your cognitive and learning skills.

Encouraging self-absorption. A UK study found that people who spend a lot of time on social media are more likely to display negative personality traits such as narcissism. Snapping endless selfies, posting all your thoughts or details about your life can create an unhealthy self-centeredness, distancing you from real-life relationships and making it harder to cope with stress.  

5 Ways to Help Kids Overcome Technology Addiction

1. Set goals for when your child can use his or her electronic devices. For example, you might schedule use for only certain times of day, or you could reward your teen with a certain amount of time on his phone once he’s completed a homework assignment or finished a chore, for instance.

2. Replace time spent on electronic devices with healthier activities. If your child is bored and lonely, resisting the urge to use her smartphone to play games or check social media can be very difficult. Have some suggestions for other ways to fill the time, such as reading a book or chatting with friends face-to-face.

3. Remove social media apps from your child’s phone so he or she can only check Facebook, Twitter and the like from a shared family computer. Remind them that what they see of others on social media is rarely an accurate reflection of their lives—people exaggerate the positive aspects of their lives, brushing over the doubts and disappointments that we all experience. Spending less time comparing themselves unfavorably to these stylized representations can help to boost their mood and sense of self-worth.

4. Limit checks. If your child compulsively checks her phone every few minutes, help her ease off by limiting her checks to once every 15 minutes, even to the point of setting a timer, if necessary. Increase to 30 minutes and even 60 minutes in time.

5. Help your child curb his or her fear of missing out. They need to accept that by limiting smartphone use, they’re likely going to miss out on certain conversations, breaking news, or new gossip. There is so much information available on the Internet, it’s almost impossible to stay on top of everything, anyway.
What to Do When Inappropriate Online Behavior Happens

What if you see that your child has some Facebook, Instagram, or SnapChat posts that you frankly feel shocked and embarrassed by? As with everything surrounding Internet use and safety, conversation is key.

"Starting with a simple, 'I saw your Facebook post... what’s up?' is a good way to get the ball rolling. Or, 'I saw some things on your wall that I’m concerned about. Let’s talk.' If you have already set the precedent that you can and do look at your child’s internet activity, there shouldn’t be much shock on your child’s part. He or she may be angry at you or feel intruded upon, but again, if this is something you have talked about before, there’s no need to react to their reaction.

In fact, you can say that this is exactly the kind of thing that you need to be talking about. Express your reasons for being concerned and reiterate your feelings about explicit behavior on or offline. This may also open up a dialogue about self-respect, setting boundaries, and privacy.

Hard as it may be, you want your tone to be open and concerned—not angry and blaming, or shocked and horrified. And you don’t want to start out by slapping on a bunch of restrictions. You’re not going to be able to have a real conversation if you do that, and kids will be more prone to do an end-run around the rules if they don’t feel that you understand them. Social media may not seem important to you, but it can seem like life or death to teenagers."

It is also important to understand the legal ramifications of risky online behavior. Many teens have been jailed and placed on probation all because of sexting. Worse, your teen could be charged with the distribution of child pornography if a sexually explicit picture of a minor is being distributed. Taking, sending, or forwarding nude photos of anyone under the age of 18, including oneself, could result in hefty legal consequences. In some states the charges for a minor soliciting child pornography are the same as for adults, not to mention it could also prevent teens from receiving college scholarships and job offers.
In reality, there are dangers that threaten our family, both from without and within. And thanks to technology today, it has never been easier for harmful outside influences to gain access to each of us, but especially to our children. We need to protect our families with vigilance.

It isn’t easy, but it requires two things: offense AND defense. Now for those of you who aren’t big sports fans, offense is when you’re trying to get something done. Defense is when you are trying to stop something from being done.

In basketball and football, offense happens when your team “has the ball” and is trying to put it in the basket for points or in the end zone for a touchdown. If baseball is your sport, your team is on offense when it is their turn “at the plate” to try to score runs. In other words, offense means taking action to score point. In all those sports, when a team is on defense, it is trying to stop the other team from scoring points.

For a family, going on offense means taking action to strengthen your family from within so it can succeed in spite of outside pressures. Going on defense means taking steps to keep harmful outside pressures away from your family in the first place. Both are needed to protect your family if you want to win consistently.

It is my hope that this book has provided you with some of the tools and strategies you need to effectively play both sides—offense AND defense—at the same time, for the well-being of your family.
Everyone knows that technology changes minute by minute. What that means to parents is that by the time you’ve figured out one app your child uses, he or she has already abandoned it and is involved in another one that you know nothing about.

Computers, tablets, and hand-held devices all have the potential to open doors for your children to places you simply do not want them to be. Luckily, there are people whose job it is to create up-to-the-minute parental control software, which makes it easier for you to do your parental job of protecting your child.

Below is a list of the best-rated options we know of for you to use as a starting place to explore the vast universe of parental control software. Most of these software programs share similar features, so it will be worth your while to explore each site to get an idea of which one feels right for you.

- **Content Watch Net Nanny** – currently considered to be the most effective parent control software available due to its advanced web filtering capabilities. It blocks access to porn, masks profanity, monitors social media, allows parental control over time spent online, and provides reports and alerts.

- **Qustodio** – in addition to web filtering capability, parents love Qustodio’s ability to set time limits on an individual app instead of blocking it altogether, and the basic service includes multiple device management.

- **Spytech Sentry PC** – while sharing many of the same features as Net Nanny and Qustodio, this software is also strong in its defense against more sophisticated teens bypassing the filters. Repeated attempts to do so will send an alert to the administrator.

The following are Apps for iOS and/or Android use:

- **Our Pact** – allows parents to set schedules for when smartphone apps are available to users, and also has an on-demand blocking feature. A child’s phone is still functional for calling and texting, but cannot access any apps when the parent has them blocked. (This is a great discipline tool!)

- **Mama Bear** – GPS location services allow parents to receive alerts when kids enter or leave a tagged location. The app also alerts administrator when user is speeding above a set limit, a very handy tool for those of us with new drivers!

- **PhoneSheriff** – In addition to the usual filtering and monitoring features, this app keeps track of any deleted content on the target device, such as texts and internet browser history, even if viewed in the incognito mode.
"TECHNOLOGY & YOUR KIDS

12 http://www.huffingtonpost.com/rachel-busman-psyd/caught-your-kid-sexting-n_b_4664367.html

5 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
6 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
7 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
8 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
9 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
10 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
11 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)
18 http://tech.lds.org/wiki/Internet_filtering_(Family_Safety)