Digital Kids Guide for Parents Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Table of Contents (click these links for faster access)

Please visit Facebook and search for the group "Digital Kids (chriswmckenna)". Once there, ask to join this closed group, where you can always find the most updated version of this document. If you don't have Facebook, send me an email (chriswmckenna@gmail.com) and I will add you to the email distribution list.

****Throughout this document, you will see me promote the MOBICIP web browser for all internet-ready devices, especially portable devices. Recently, I agreed to be an advocate for their product, because I've tested many filters, and it just does the best job. It's what I use on my own portable devices! There's no perfect filter out there, but Mobicip passes all of the major tests. If you decide to choose Mobicip after hearing the Digital Kids presentation, please click this link so that they know I gave the recommendation: http://www.mobicip.com?tap_a=478-0cfcfe&tap_s=1556-b94429 Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Digital Kids Opening

I'm passionate about protecting young eyes from online dangers. I was exposed to pornography in elementary school, which led to an adult addiction, and I don't want ANY child to fall into this trap. It is an issue that does not go away easily. The average age of the first hard-core pornography exposure is currently 10.7! If your son or daughter has access to a laptop, tablet, iPod or smartphone, you'll want to be very involved in their usage. There are many doorways to inappropriate material.

These are realities that we must accept when it comes to technology:

- **The influence of technology** over our lives is going to continue to increase drastically.

- At some point, **almost every child will be exposed to something harmful on the internet.**

- Because the internet's purpose is to **provide access**, there will almost always be a way to beat the controls we try to put around it.

- It's just not the same as when you grew up! According to psychologist Al Cooper, the internet is fueled by **availability, affordability, and anonymity** for most things people crave.

The statistics are mind-numbing:

- The most popular category of sexual searches is the word "youth" (Covenant Eyes 2013 Porn Stats p.7)

- According to Juniper Research, by 2017, a quarter of a billion people will use their MOBILE or tablet device to access adult content (Covenant Eyes 2013 Porn Stats p.9).

- Most experts estimate that the average age of first pornographic exposure on the internet is 10.5-11.

- Approximately 43% of high school students experience some form of cyberbullying (http://www.a4kclub.org/get-the-facts/bullying-statistics).

The purposes of this document are the following:

- To **PROTECT** as many young eyes as possible from the dangers lurking in internet-ready devices.

- To **SAVE** parents valuable time by doing the research for them.

- To **EXPLAIN** the purpose and risk associated with the different APPS used by kids today (see "APPS" section below)

- To **SHOW** parents how to use filtering and monitoring tools to prevent harmful exposures (see the "Web Filtering and Monitoring" section below).

This document focuses on Apple (iPhone, iPad, iPod) and Android (Samsung, HTC, others) mobile devices. **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

APPS Explained

APPS rule the smartphone and tablet world and are downloaded onto devices to perform a specific function. Almost anything popular from the internet has a related APP, but the reverse isn't always true. For example, there is a "snapchat.com" that explains the company, but the functionality that kids desire is only in the APP.

Throughout the APP section, I mention both Mobicip (web browser) and OpenDNS (router filtering), which when used in tandem, provide an extremely solid, inexpensive web filter and monitoring solution. More on these solutions in the "**Layers of Digital Protection"** section below.

The rule of thumb with APPs is this – if it allows user-controlled content (pictures, videos), it will ALWAYS have a dark side.

KiK (accessible only as an APP)

Description: KIK is a smartphone/tablet application for instant messaging. Most use KIK as an alternative to SMS text messaging due to its integration with other multi-media (You Tube, Photo Bucket, etc.) and other social media platforms (e.g., Instagram, Facebook, Twitter, Tumblr, etc.). People who use KIK as referred to as "Kiksters" and there are over 100 million Kik users as of March 1, 2014.

Category: instant messenger, social networking

APP Store Rating: 17+ ("frequent/intense mature/suggestive themes")

Risks: There is an internet browser within KIK, giving access to any website, along with an image search, YouTube video search, etc. Conventional web filters you might download onto a mobile device don't have any control over these capabilities within the APP. The greatest risk to your child's safety and privacy is the ability to invite people via social networks. With the click of a button, a child can reach out to the public communities on Facebook, Twitter, Intagram, Tumblr and others with the message "Kik me". This begins a new instant message conversation between the sender and the recipient, whoever they may be, making it a perfect place for individuals with bad intent to troll for unsuspecting victims. A significant law-enforcement issue with Kik is that it's a Canada-based company, making it difficult and slow for US-based authorities to pursue inappropriate activity. Finally, there are no records for parents to review and chats are easily deleted.

How to monitor: For both Apple and Android devices, monitoring is VERY limited. Assuming you know their Apple ID and Kik activity is included in the iCloud back-up settings, TeenSafe (paid service – 1-week trial and $14.95/month after that) can show you sent and received texts. **I'm still running some tests on TeenSafe's service (2/1/15).** OpenDNS can block the web search feature within Kik, but the YouTube and Image search "add-on's" within Kik still allows some searching for inappropriate content. OpenDNS cannot prevent your child from advertising his/her Kik username via social media, if he/she has an account with Facebook, Twitter, Instagram, Tumblr, etc. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted. Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Other instant messaging APPS include WhatsAPP (green logo) and Viber (purple logo). Neither has the functionality of Kik and aren't as popular with teens. Neither can be monitored with OpenDNS – the only option seems to be using a paid filter or monitoring service. More on these solutions in the ***Web Filtering and Monitoring*** section below.

Snapchat (accessible only as an APP)

Description: A couple of Stanford students created this APP, which combines the best of texting, pictures and video. Users "snap" an image or video, add a caption, and send it to friends, who can view the photo for a specified period of time before it disappears (unless they take a screenshot). With the addition of the "Snapchat Story" feature, "snaps" can be stored for up to 24 hours. It can be an extremely fun way to interact with friends as you share short, spontaneous moments. In November 2014, Snapchat added "Snap Cash," which allows users to send money to each other using Square Cash's technology (the little white square you've probably swiped on the top of an iPad at your favorite coffee shop - that's Square Cash technology).

Category: photo sharing, video sharing, social networking

APP Store Rating: 12+ ("infrequent/mild alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, sexual content and nudity")

Risks: The most obvious risk is the deception of secrecy and that "no one will know" because the photos supposedly disappear. Both Apple and Android devices allow for users to take a screenshot, thereby preserving the potentially inappropriate image forever and various claims have been made by security agencies that they were able to recover photos even after they "disappeared". It has earned a reputation as a sexting haven. Scorned lovers use preserved Snapchats photos as "revenge porn" against their former lovers. There's no evidence to support this since it's so new, but the Snap Cash feature could be used to offer money for inappropriate photos.

How to monitor: the Snapchat APP can't be monitored with conventional web filters and is not stopped by OpenDNS. In Snapchat's settings, you can only allow "My Friends" to send snaps to the account (otherwise, anyone can send a picture). Also, Snapchat does have a "block" feature to block certain friends if necessary. Over 2 million people (mostly parents) are now using a monitoring service called mSpy, which is pricey ($199.99/year), but it's comprehensive, and the only solid tool for Snapchat on the market. In addition, the premium service monitors all internet browsing, texts, emails, SKYPE, What's APP, iMessage, Viber, provides GPS location services, and more. Note – mSpy is a monitoring tool and not a filtering tool, so it's not going to prevent inappropriate material but it will show you everything happening on the device. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted. Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Vine (as an APP or website, https://vine.co/#/feed)

Description: Vine is a way to create short, looping videos, which can be easily shared.

Category: video sharing, social networking

APP Store Rating: 17+ ("infrequent/mild alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, frequent/intense sexual content and nudity, etc.")

Risks: Vine has become a place to post short, looping inappropriate videos, which can be easily accessed through its search feature, even without a registered account.

How to monitor: the Vine APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "video sharing" category. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted.**

Tumblr (accessible as an APP or website, www.tumblr.com)

Description: Tumblr is sometimes touted as a micro-blogging platform, but as it says on its own website, "Tumblr lets you effortlessly share anything," including text, photos, videos, links, music, with complete customization capability. The day this was typed, there were over 102,000,000 posts made on Tumblr.

Category: blog, social networking

APP Store Rating: 17+ ("frequent/intense sexual content or nudity")

Risks: The APP store rating says it all. The ability to post anything means that people post anything. And, you don't need an account to access everything that is posted. Just download the APP and search for keywords.

How to monitor: the Tumblr APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "blogs" category. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted.**

Ask.fm (as an APP or website, http://www.ask.fm)

Description: a Latvia-based, social-media company, where people ask other users questions with the option of anonymity. In 2013, there were over 80 million world-wide users. It's estimated that 25% of teenagers in the United States have used Ask.fm in the past 30 days in some way.

Category: social networking

APP Store Rating: 12+ ("infrequent/mild cartoon/fantasy violence, alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, sexual content and nudity")

Risks: Ask.fm has come under scrutiny due to its connection to cyber-bullying, particularly 4 teenagers, including sisters, ages 13 and 15 from Ireland, whose suicides have been linked to comments made on the site. Ask.fm is integrated with Facebook and Twitter, easily sharing what is posted on Ask.fm on these sites. One user can block another user, however a blocked person can still access any profile to view other interactions. Ask.fm is located in Latvia, making legal requests from the United States time-consuming.

How to monitor: OpenDNS does not block the APP or the website, even when the "social networking" category is blocked. The website can be blocked through Apple and Android's system restrictions**.** The ability to **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

be asked questions anonymously is the default feature of Ask.fm. Teens should disable this feature in order to avoid questions from users wishing to remain anonymous. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted.**

Facebook (accessible as an APP or website, www.facebook.com)

Description: Not much needs to be said. With over 1 billion users, 350 million photos uploaded daily (over 250 billion to date!) it is the king of social media.

Category: social networking

APP Store Rating: 4+, although users are supposed to be at least 13 years old in order to comply with the Child Online Privacy Protection Act (COPPA), which applies to websites and online services that collect personal information.

Risks: both privacy and exposure to inappropriate content should be concerns for parents. Teenagers typically overshare private information, so parents must have intentional conversations around what should and shouldn't be shared. The following link provides guidelines for enhancing user privacy:

http://www.insidefacebook.com. There are also endless numbers of inappropriate people, photos, pages, and APPS that can be accessed through Facebook with a simple search.

How to monitor: the Facebook APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "social networking" category. If you want access to Facebook, yet want to monitor your child's Facebook activity, you should know their username and password, be their "friend" and make it clear that you are watching. The MamaBear APP is also an excellent tool for monitoring the "Big 3" (Instagram, Twitter and Facebook). It's FREE and will give you a newsfeed of activity in all 3. You can also use a monitoring service, similar to Family Signal (www.familysignal.com) and for $4.99/month, you can receive email and text alerts for inappropriate Facebook, Twitter and Instagram activity. I've tested this service, and it works well, **assuming you know all active accounts**.

You Tube (accessible as an APP or website, www.youtube.com)

Description: The king of video sharing websites, part of the Google family. The statistics around YouTube are mind-numbing; with over 100 hours of video uploaded to YouTube every minute (do the math!).

Category: video sharing

APP Store Rating: 12+ ("infrequent/mild cartoon/fantasy violence, alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, sexual content and nudity," etc.)

Risks: With so much material, there's just so much inappropriate material out there. And, it's not hard to get to it.

How to monitor: the YouTube APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "video sharing" category. But, most parents will probably be convinced by their child to allow some YouTube access, and there's no in between with OpenDNS – it's either blocked or open. Within the APP and the website, YouTube's own search parameters can be set to either "Don't filter" or "Strict" – and **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

parents will want to keep "strict" selected. The problem with both the APP and the website is that the search parameters are easily changed. And, if changed, only Mobicip filters videos within the YouTube site.

Instagram (accessible only as an APP)

Description: A simply way to capture and share photos and videos with friends, utilizing a variety of custom photo filters to enhance and beautify life's moments. Instagram is probably the most popular "social media doorway" for young people.

Category: photo and/or video sharing

APP Store Rating: 12+ ("infrequent/mild alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, sexual content and nudity," etc.)

Risks: Because it's built on pictures and videos, there is plenty of inappropriate content. Even though Instagram touts prevention of inappropriate content, there are many ways to beat their controls. The hashtag feature just creates a repository of specific themes for people to troll, i.e., #girls, #kikme, #snapchatnudes, etc.

How to monitor: the Instagram APP can't be monitored with conventional web filters and is not stopped by OpenDNS. If you want to monitor your child's Instagram activity, you should know their username and password, be their "follower" and make it clear that you are watching. The MamaBear APP is also an excellent tool for monitoring the "Big 3" (Instagram, Twitter and Facebook). It's FREE and will give you a newsfeed of activity in all 3. You can also use a paid monitoring service, similar to Family Signal (www.familysignal.com) and for $4.99/month, you can receive email and text alerts for inappropriate Facebook, Twitter and Instagram activity. I've tested this service, and it works well, **assuming you know all active accounts**. Also, if you want to control who can see posts, set the account settings to "private". This makes would-be followers ask permission to follow, and only allows followers to see posts (instead of the general Instagram public). Since this is usually a doorway APP into the social media world for tweens and middle school students, parents just need to understand that due to user controlled content, Instagram has a dark side and shouldn't be taken for granted.

Twitter (accessible as an APP or website www.twitter.com)

Description: A way to share your life's moments 140 characters at a time. It is one of the top-10 most popular websites globally. Registered users can read and post messages or "tweets" while unregistered users can only read messages.

Category: social networking

APP Store Rating: 4+ (but, don't believe it – see Risks)

Risks: The news is full of sports figures and celebrities who have used Twitter to "vent" and say regretful things. Twitter gives potential cyber bullies a fast way to say dumb and hurtful things. Additionally, anyone can get access to pictures that people have posted through their Twitter account. If you search for a name, you will see names and profile pictures and from there, it's easy to see pictures attached to each profile and Twitter is rife with adult stars who post everything with pictures – it is flying under the radar in terms of pornographic material but is very accessible and is being used by more and more middle schoolers. The hashtag feature just creates a repository of specific themes for people to troll. **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

How to monitor: the Twitter APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "social networking" category. The MamaBear APP is also an excellent tool for monitoring the "Big 3" (Instagram, Twitter and Facebook). It's FREE and will give you a newsfeed of activity in all 3. You can also use a paid monitoring service, similar to Family Signal (www.familysignal.com) and for $4.99/month, you can receive email and text alerts for inappropriate Facebook, Twitter and Instagram activity. I've tested this service, and it works well**, assuming you know all active accounts.** If you delete the Twitter APP and force use through the web with Mobicip, you can effectively block the Twitter profiles with adult content OTHER THAN their related thumbnail pictures, which might be inappropriate.

Netflix (accessible as an APP or website www.netflix.com)

Description: Provider of streaming movies and TV episodes.

Category: movies, entertainment

APP Store Rating: 12+ (this is actually laughable, since many MA rated movies are easily accessible)

Risks: Netflix provides access to almost any movie. Parental controls really don't prevent a kid watching inappropriate movies, since they can be easily changed.

How to monitor: the Netflix APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "movies" category (but, this category also blocks the APP store). Alternatively, parents can go to the Netflix "Help Center" for instructions on how to adjust maturity levels and create user profiles to match your situation.

Whisper (accessible as an APP or website http://whisper.sh/)

Description: a way to anonymously share feelings with pictures and words, and if so desired, connect with individuals through a messaging option. The APP store description says this, "build lasting, meaningful relationships in a community built around trust and honesty".

Category: social networking

APP Store Rating: 17+ (infrequent/mild profanity or crude humor, suggestive themes, alcohol, tobacco, or drug use)

Risks: Plenty of suggestive, sexually charged material in the form of provocative pictures and words. The ability to connect with others with FREE private messaging is inherently risky.

How to Monitor: the Whisper APP can't be monitored with conventional web filters and is not stopped by OpenDNS.

Textfree (accessible only as an APP)

Description: the original, free SMS texting app that gives you your own phone number, free, unlimited text messaging, plus calling to any phone, including landlines and non-smartphones, in the US and Canada. Friends don't need Textfree to receive calls/texts. This is commonly used by kids who have iPods with Wi-Fi capability.

Category: lifestyle **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

APP Store Rating: 4+

Risks: inherent risks come with any texting app. Parents just have to monitor appropriate usage.

How to Monitor: The Textfree account can be set up with parent email information which parents can use to access web monitoring for sent and received texts. Read this article for details: http://internet-safety.yoursphere.com/2011/08/an-easy-way-to-introduce-and-teach-your-children-responsible-texting/

Yik Yak (accessible only as an APP)

Description: Created by 2 Furman graduates last fall, it was intended to become a virtual bulletin board, using GPS location data to bring comments from other near-by users into the feed.

Category: social networking

APP Store Rating: 17+ ("frequent/mild alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, sexual content and nudity," etc.)

Risks: Recent cyberbullying incidents in Chicago and Georgia, and a bomb threat in California, show how something innocent can always be used for evil. Fortunately, Yik Yak did the right thing, and is now creating geo-fences around middle and high schools that will prevent the APP from being used when a smartphone's GPS sees that they're within the "fence". But, inappropriate usage can occur anywhere.

How to Monitor: the Yik Yak APP can't be monitored with conventional web filters and is not stopped by OpenDNS.

I've included icons for the Google and BING APPs. I mention these, because even if you set Apple's or Android's manufacturer "Restrictions" on your portable device to "block adult content", this only works when you're using Google, Bing and other search engines **through the browser (e.g., Safari, Chrome)**. These restrictions **don't** apply to the AAPS! As mentioned above, just try to avoid using APPS for things that can be accessed through a filtered browser.

Pinterest (accessible as an APP or website www.pinterest.com)

Description: One of the most popular social media sites on the planet right now, where people "pin" creative ideas on their "boards" which are shared.

Category: social networking

APP Store Rating: 4+ (but, don't believe it – see Risks)

Risks: Yes, there are amazingly beautiful and creative things people have shared, but with any site that allows users to control uploaded content, there will be inappropriate items, and Pinterest is no different. If using the APP, you must log-in in order to search content. If using the web, you DON'T need a log-in to search content (which is an issue). If you directly type in an inappropriate search word, the site will say, "we don't allow things that are inappropriate" but that's just not true. There are TONS of inappropriate pictures that just aren't tagged with any inappropriate words that would be flagged by Pinterest's filters. **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

How to Monitor: the Pinterest APP and website can be effectively blocked with OpenDNS on both Apple and Android devices, using the "social networking" category. If you delete the Pinterest APP and force use through the web with Mobicip, you can effectively block most (but definitely not all) inappropriate searches.

Omegle (accessible as an APP or website www.omegle.com)

Description: is a free online chat website that allows users to communicate with others 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" (or "Stranger 1" and "Stranger 2" in the case of Spy mode).

Category: social networking

APP Store Rating: 17+ ("Infrequent/mild profanity or crude humor, frequent/intense sexual content or nudity")

Risks: Well, the ability to be paired up with anyone with any intent speaks for itself. Even the creators of Omegle warn that anyone under 18 using the APP should be monitored by parents. At the end of a "chat," users are given the option to "save the log" preserving any sensitive/private information that might have been shared. What typically happens is someone will start a chat and offer their KiK username where the conversation continues with all of Kik's features.

How to Monitor: It should be blocked by Open DNS' "social networking" category, but in my testing, I can't get it to block, and it's still usable with Open DNS active. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted.**

Pheed (accessible only as an APP)

Description: Pheed is this combination of everything – Facebook, Instagram, Vine, Tumblr – all smashed into ONE social network APP. It's specifically aimed at a younger audience than Facebook, where everyone's parents now have accounts. Pheed combines text, video, images and audio, and includes a live broadcast option. Pheed is very new and still not very popular but it's very much worth watching for.

Category: social networking

APP Store Rating: 12+ ("infrequent/mild alcohol, tobacco, drug, mature/suggestive themes, profanity or crude humor, sexual content and nudity," etc.)

Risks: The APP store rating is too low – it should be 17+ since inappropriate content is just a few clicks away. This APP combines all of the features that promote inappropriate use – hashtags, user-controlled content, video, etc.

How to Monitor: Pheed is blocked with Open DNS' "social networking" category. **Parents should take extreme caution when deciding if their kids should use this APP based on the risks noted. Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Layers of Digital Protection

It is extremely difficult to find the "one tool" that does everything that I would like, which includes an effective and customizable web filter, activity monitoring (including text, social media), and reporting. A big issue lies in the APPS versus the websites. ***Additionally, relying only on a filter to enforce responsible digital behavior won't work. Remember our realities? The web is an ACCESS tool, and someone with enough motivation will find a way to beat the controls.*** But, if a good web filter is accompanied by parents who are engaged, informed and encourage responsibility, you have a great chance at being successful.

Remember, this is our goal: prevent 90% of the junk with filters and monitor the other 10% for searching patterns that can lead to productive conversation.

Web filtering and monitoring Levels

Web activity can be filtered and monitored at a couple of different levels, including:

☐@ the location level

☐@ the wireless router lever

☐@ the desk/laptop computer level

☐@ the mobile device level

@ the location level

• Keep all portable, internet-ready devices out of bedrooms; have a bedtime "turn in" time for devices; **all** devices are used in very public places.

• Talk to parents of friends to better understand the rules around portable devices at those homes so that you can determine what, if anything, you need to share about your expectations.

• Talk to school and church administrators.

@ the wireless router level

***I recommend installing OPEN DNS onto your home's wireless router (www.opendns.com). This goes a long ways towards preventing 90% of the junk from getting through and the monitoring reports help with the other 10%), and it's FREE!** This is necessary to that ANYONE surfing your Wi-Fi is subject to some filtering. It's free and easy and it essentially uses Open's servers to filter out the bad stuff using categories you can customize, depending on your family's needs. **Note: for the 3 major search engines (Google, Yahoo, and Bing), OpenDNS has major limitations for IMAGE searches. It does well for many inappropriate websites, but a handful still get through. If you use OpenDNS as your ONLY filter, I recommend that parents block major search engines other than Google on their devices using Open's "always block" list, then lock Google's "safe search" option, and enable the Open DNS "monitoring reports" so that you can see all activity. For your own children, I always recommend all layers of protection (location, router and device, as explained in this document), but for visitors (i.e., friends), using OpenDNS will help if they have no controls on their devices. **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Remember, you might want to change the category settings in OpenDNS for that sleepover. Meaning, maybe you've controlled image searches on your son's iPod by adding Mobicip. But, chances are most kids will come with portable devices where they have access to other search engines. So, you might want to add things to the black list on OpenDNS that you don't have to worry about with your son, or block the category "search engines" (which still allows Google). **At a minimum, for every sleepover, have a conversation with the group to let them know of your home's rules for appropriate usage.**

Google special note – The best way to control Google, regardless of what filtering you use is to use Google's "lock safe search" option, which you can use only if you have a Google+ account. Here are steps for locking Google safe search: https://support.google.com/websearch/answer/144686?hl=en&rd=2

You can also unplug the router at night, especially during sleepovers, to prevent unwanted night-time usage (which is when most trouble occurs).

****Special Note for U-VERSE (AT&T) Customers:** unplugging the router at night presents issue because that will disable everything. Also, AT&T won't allow OpenDNS to be installed on the router you get with U-VERSE, but there is a way around this by installing a second router. Read this article for details: http://forums.att.com/t5/Residential-Gateway/U-verse-for-BUSINESS-2Wire-3600HGV-bridge-mode-or-another-AT-amp/m-p/2707755#M182

@ the lap/desktop computer level

There are some very good desk/laptop filters and a few that I recommend based on price and functionality include: K9 (free) web filtering and Mobicip (free). Since desktops have been around a while, the related filtering solutions are good. K9 has filtering weaknesses with Twitter searches and also Pinterest, so you will want to monitor activity for time spent in these two areas. I (Chris) use K9 filtering on our home laptop along with Open DNS for the home wireless network.

Here is an article that reviews desk/laptop parental software solutions if you want something other than the two I've previously mentioned: http://parental-software-review.toptenreviews.com/ .

@ the mobile device level: iPod Touch, iPhone or iPad

The biggest reasons kids ask for an iPod touch are for downloading and listening to their favorite music, and for texting with their friends. Anyone with an iPod can iMessage (Apple's word for text) anyone else with an Apple device while connected to Wi-Fi. Unlimited and free! Here is Apple's article explaining how iMessage works: www.apple.com/ios/messages/ . If you want to monitor your kid's iMessage activity, here is an article with some savvy tips: http://www.ianswerguy.com/monitor-text-messages/ . **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

But, if kids want more text functionality and the ability to text with friends who do NOT have an Apple device, then most parents turn to a texting app, like Textfree, KIK, WhatsApp, or Viber. If you select TextFree (which I recommend over the others), be sure to enable the "send an email" functionality so that you can monitor Textfree activity and you can also monitor sent and received texts over the web. Follow this link to for instruction on setting the right restrictions: http://internet-safety.yoursphere.com/2011/08/an-easy-way-to-introduce-and-teach-your-children-responsible-texting/

The iPod Touch, iPhone and iPad all have access to the internet and the APP store, and so Apple's manufacturer "restrictions" should also be used. ***Enable Apple's Restrictions (this goes a long way in preventing 90% of the junk getting through and when you enable restrictions, browsing history cannot be deleted, preserving the 10% for searching patterns and conversations).** Please read through all of these bullets:

☐Read the following in order to view screenshots for getting started: http://www.howtogeek.com/177366/how-to-lock-down-your-ipad-or-iphone-for-kids/ . Once you initiate Apple's "Restrictions," you have control over adding and deleting APPS (which is important).

☐Eliminate all APPS that allow web access. For example, delete the Google search APP and force use of Google in the Safari browser.

☐BUT, this is not a failsafe lock-down! Within the Safari Browser, you have the option of using 3 different search engines: Google, Bing or Yahoo (click on "Settings" icon, then find the Safari icon and click – you will see "Search Engine" at the top with the 3 options). Even by "limiting adult content" under "Restrictions," the safe search options can be inexplicably changed from "safe" to "none" on www.bing.com giving access to **anything**. For Yahoo and Google, once "limiting adult content" is selected under "Restrictions," the safe search settings cannot be changed.

☐Another drawback is that Apple "Restrictions" don't limit access to inappropriate videos in YouTube and Vimeo, and image searches in non-traditional search engines (e.g., www.webcrawler.com). So even if you have Yahoo set as Safari's default search engine, you can switch it to Web Crawler.

☐Because of these holes, if you choose to just use Apple's Restrictions, then at a minimum, block certain search engines. Within Settings, click "Restrictions", then "Websites" then add these to the "never allow" section:

o www.bing.com

o www.webcrawler.com

o www.excite.com

o www.zoo.com

o www.lycos.com

o www.duckduckgo.com

o www.tumblr.com (micro blogging – see APP section for details)

o www.altavista.com

o www.infospace.com

o www.blekko.com

o www.contenko.com

o www.alhea.com

o www.baidu.com (Chinese search engine)

o www.reddit.com (doorway to Imgur images and tons of inappropriate stuff)

o www.imgur.com (image dump)

☐ **In my view, Apple devices simply require an additional level of security, which is why I highly recommend Mobicip to be used as the web browser for all portable devices (in the APP store and at www.mobicip.com – this REPLACES Safari on Apple devices and Chrome on Android devices). The combination of Apple's restrictions + Mobicip + Open DNS on the router goes a long way in preventing 90% of the junk from getting through and being able to monitor the other 10% for searching patterns.** The free version is great, and for an additional $39.99/year (up to 5 devices), you can go "premium" (what I use) and customize filtering categories, enforce time limits, create a black/white list for websites, block certain keywords, monitor what APPS are on the device, and have usage reports emailed to you. It's the one that handles YouTube videos well – allowing you to use YouTube, but blocking objectionable material. Mobicip uses 3 filtering levels, which you can customize: elementary, middle or high school level. Mobicip becomes the web browser, replacing Chrome, Safari, Firefox, etc. (there are instructions within Mobicip for turning off Safari on Apple devices, which is critical).

o ****Mobicip Limitations:** Mobicip struggles some with blocking keyword searches in Twitter, but every solution strugglers mightily here. For filters that allow Twitter use (some block it completely), Mobicip does better than anything else I've seen.

o If you decide to use Mobicip, can I ask a favor? Please use this link to let them know that I recommend them: http://www.mobicip.com?tap_a=478-0cfcfe&tap_s=1556-b94429

Other monitoring services

Maybe due to your specific situation, you might want to monitor more than just internet activity, including photos, videos and texting. I recommend the following, which are shown in descending order of "intensity":

☐ Talk to your cellular service provider (i.e., AT&T, Sprint, Verizon) to see what parental controls they might provide "at the source" of the 4G signal.

☐ **Family Signal** (www.familysignal.com, $4.99/month) – allows tracking of suspicious activity on Facebook, Twitter and Instagram, looking for indications of sexual, bullying or profane language. I tested this service for a month and it was easy to set up (assuming you know your child's account information) and effective.

☐ **MamaBear Family Safety APP** (www.mamabearapp.com, free version, $14.99/3-month premium, $24.99/6-month premium) – a step more than Family Signal, providing location services, monitoring of the "Big 3" social media sites (Facebook, Instagram and Twitter), driving speed, and more. I tested this service and it was easy to use, and effective.

☐ **TeenSafe** (www.teensafe.com, offers a free, 1-week trial, and $14.95/month afterwards) – a step more than MamaBear, tracking mobile activity for calls, texts, Facebook, Instagram, Kik messages received and sent. **I'm still working through a 1-week trial as of 2/1/15.**

☐ **mSpy –** (www.mspy.com, see pricing here: http://www.mspy.com/buynow.html). mSpy is the ultimate in monitoring smartphone activity. I already mentioned this service above under my explanation of the Snapchat APP, since it's the only service that monitors Snapchat activity. The issue some will have is that in order to monitor Snapchat, Viber, What's APP and other social media APPs, an Apple device will need to be "jailbroken" and you will need physical access to the device for 5-10 minutes to complete the

installation. To “jailbreak” an iPhone means to allow certain third party software, like mSpy to have “root access” to the iOS. There are risks associated with a “jailbreak” which you can read about on mSpy’s website.

@ the mobile device level: Android and Kindle

Manufacturer lock-down features for Android devices

- Please read the following: http://content.mobicip.com/content/how-setup-parental-controls-android

- Since I do not have an Android device, I have not tested the strength of their manufacturer settings. After reading the Mobicip article above, please “test” the settings looking for some of the “Web Filtering Minimum Criteria” listed above.

Manufacturer lock-down features for the Amazon Kindle

- Please read the following for the Kindle: http://blog.laptopmag.com/how-to-set-parental-controls-on-the-kindle-fire-hd

- Note: there are no web filters that you can put in place over SILK, the Kindle browser. Therefore, you may choose to simply remove SILK from the device. I highly recommend setting up parental controls to don’t allow APP downloads unless the parental control password is provided.

Everything I mention above in the Apple section related to using Mobicip as the web browser and “Other Monitoring Services” (Family Signal, MamaBear, TeenSafe) also applies to Android devices. Other information specific to Android includes:

- www.txtwatcher.com (3 pricing tiers, including a free version) – for Android devices only, a simple, easy way to monitor SMS texting activity.

@ the game system level: X-box or Play Station

Both of these devices rely on the wireless signal in your home, which goes back to having filtering controls at the router level. There are also parental controls that you can use on the consoles themselves (i.e., for controlling games with certain mature ratings), which are outlined in the following links:

http://support.xbox.com/en-US/xbox-360/security/xbox-live-parental-control

https://support.us.playstation.com/app/answers/detail/a_id/5097/~/ps4-parental-controls **Digital Kids Guide for Parents** Updated: February 1, 2015 chriswmckenna@gmail.com **All updates since last version are highlighted in yellow.**

Privacy Concerns

Absent any action by you, the default settings on your portable device are likely set to gather geo-location information, which is tagged to photos and posts. I recommend taking a few minutes to review your portable device’s

location controls to make sure they are what you desire. You can access privacy settings in an Apple device by following the pictures above, and also in the “Restrictions”.

Samsung Galaxy s4: http://blog.laptopmag.com/turn-off-galaxy-s4-location-services

HTC: http://www.htc.com/us/support/htc-one/howto/365673.html

I won’t list the “how-to” privacy steps for every device, but they are easy to locate on the web.

Closing Remarks

Remember one of our realities: the internet’s purpose is to provide access, therefore someone will always figure out a way to beat the controls. But, my experience shows that parents who are **observant, engaged, and informed** often have children who learn how to handle technology **responsibly**.

Other resources for parents:

☐Here is an excellent tool for setting expectations with kids for on-line safety: http://www.aplatformforgood.org/pages/online-safety-cards

☐This white paper gives an in-depth explanation about the draw to pornography. It is EXCELLENT (and it’s a Michigan-based company in Owosso): http://www.covenanteyes.com/resources/heres-your-copy-of-the-porn-circuit/

☐A rather graphic, yet very informative Ted Talk on the long-term effects of pornography on young men: https://www.youtube.com/watch?feature=player_embedded&v=wSF82AwSDiU

☐A summary of sexting laws by state: http://www.cyberbullying.us/state_sexting_laws.pdf