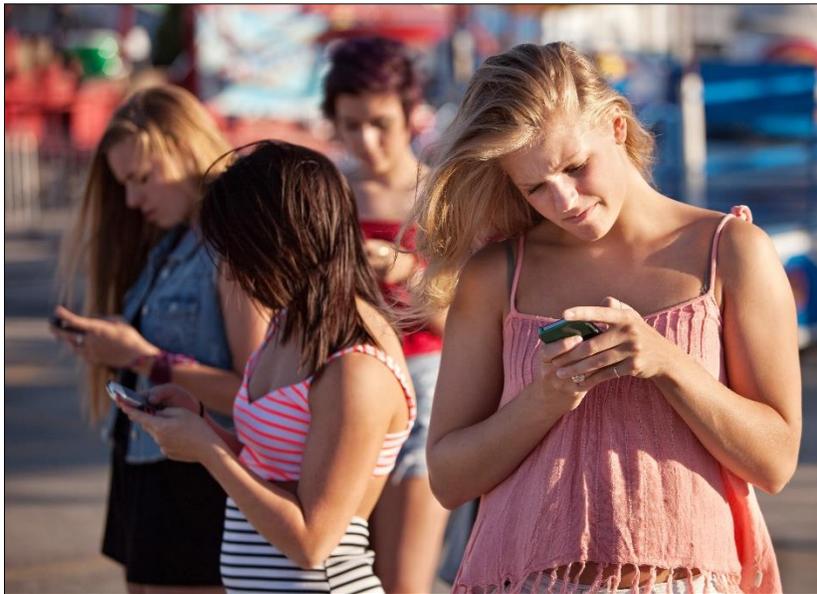


# Digital Communication, Online Activity, Smartphones, and More: How Can We Protect our Kids and Teenagers?



by Alison Meredith

## **WARNING:**

**This whitepaper is for adults. This is not for teenagers or kids.**

- This report includes explicit sexual references.
- This publication contains detailed information about how cybercriminals work, which may unnecessarily scare teenagers and kids.

## **Disclaimer**

The information and suggestions contained herein are provided by Holston IT as a free resource. The author makes no claim or guarantee that implementing the advice in this paper will protect kids or teenagers. This information is not intended as legal advice and is provided without warranty. The reader assumes all risk for reliance on any of the information in this document.

## **Permission to Share**

Further distribution of this paper is permitted if the footer is retained, the contents are unedited, and the distribution is free to others. Free distribution of excerpts is also permitted if the footer, containing a link to view the report online in full, is retained.

## **Links**

Everything underlined in this paper is a direct link to further information. All links work, as of its publication on October 3, 2019. However, websites frequently rearrange content and break links. If you find a broken link, please email the author [alison@holstonit.com](mailto:alison@holstonit.com), referencing the paragraph with the broken link.

Links can be accessed easily by reading this online, at [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids). However, a full list of URLs referenced in this paper is also listed in the addendum.

## **Credits**

Sources have been credited by directly linking to them where they are quoted. For people reading a printed copy of this, an addendum listing all links is provided. Any omission of credit is accidental; if you find such, please contact the author at [alison@holstonit.com](mailto:alison@holstonit.com) or [www.linkedin.com/in/alisonmeredith7/](https://www.linkedin.com/in/alisonmeredith7/) so she can correct it.

Special thanks to the following friends who provided valuable insights as the author crafted the final version of this report: Danielle Smith, Lynette D'Avella, Carroll Sue Priddy, Anna Manley, [Ruth Grunstra](#), and Julie Garner.

## **Additional Information: A Dozen Three-Minute Video Tips**

In the spring of 2019, Alison did a series of video tips regarding this topic, which were posted to the [Holston IT Facebook page](#) and to [the Holston IT Blog](#). Much information in those short videos did not make the cut into this whitepaper, so they are a source of additional information. You can [view them all here](#).

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.



This paper is a free resource. Further distribution is permitted if this footer is retained and the contents are unedited. [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids) [www.linkedin.com/in/alisonmeredith7/](https://www.linkedin.com/in/alisonmeredith7/) Page 2 of 28

## About Alison Meredith

Alison earned a BS from Virginia Tech. She taught Mathematics at Dudley High School in Greensboro NC, Dobyns-Bennett High School in Kingsport TN, and North Andover High School in North Andover MA. In 1997, she was one of only ten teachers nationwide to receive the Future Leaders Award from the National Council of Teachers of Mathematics.

She paused her professional work to be a stay-at-home mom. She says of those years, “The skills I gained are too numerous to list, and the pay was priceless.”

Alison has been co-owner of Holston IT since the beginning, but she took on a more visible leadership role starting in 2012. In her words, she was recruited to “serve as a translator for the geeks.” She directs client communications, sales, and marketing; she also helps medical offices comply with HIPAA regulations.

Alison is an Amazon Best-Selling author. Her first published book, [You are the #1 Target](#), is a collaboration with other leaders in the IT industry, to help business owners protect themselves from cyber-threats. You can [buy the book here](#); the authors are donating all their royalties to St. Jude’s Children’s Hospital.



Alison is actively involved in the [Medical Group Managers Association](#), [FIRST Lego League](#), [First Presbyterian Church in Johnson City](#), and her [local Boy Scout Troop](#).

## About Holston IT

Tim Meredith, a Microsoft Certified Systems Engineer, founded Holston Information Technology Company in 2008, with a vision to provide enterprise-level cybersecurity, fast response, and friendly service to businesses. The Holston IT team currently has over 15 employees and serves clients throughout Southwest Virginia, the Tri-Cities of TN, Panama City FL, and Knoxville TN. They specialize in providing cybersecurity and compliance solutions for businesses with strict regulatory requirements and security needs.

The Holston IT Team has two main ways to serve its clients: either by being the [CIO of businesses](#) which outsource all of their technology needs, or by working alongside IT managers in [Co-Managed IT](#) partnerships. Holston IT provides secure [email](#), [backups](#) with business continuity, [virtualization](#), hassle-free [compliance solutions](#), and more. Some people see technology as an expense; [Holston IT clients](#) instead view technology as a leverage to increase profitability and employee productivity.

In July of 2016, Holston IT was [featured on the cover of Business Solutions magazine](#) for their fast growth, excellent client service, and expertise in serving businesses which must comply with HIPAA.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.



This paper is a free resource. Further distribution is permitted if this footer is retained and the contents are unedited. [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids) [www.linkedin.com/in/alisonmeredith/](http://www.linkedin.com/in/alisonmeredith/) Page 3 of 28

## Why Is This So Hard?

The world has changed.

The *pace* at which the world has changed has also changed—in fact, it has increased exponentially.

For most of human history, a young adult aiming to increase his professional skills or be a better parent to his children could grab onto the same tools used by not only his parents but also his grandparents. Until just a few hundred years ago, even the tools used by his great-grandparents would have come in handy. But today, things change faster.

Let's consider telephones as an example—take a quick moment and think about this:

- What was your grandparents' telephone like, when they were raising your parents?
- What was *your* household phone like, when you were a kid?
- Do you remember how new and exciting cordless phones were? A phone you could *take anywhere in the house*?
- When did you see a cellphone for the first time? Did you get to see one of the first ones, the size of a suitcase?
- When did you decide to take the jump from a “dumb phone” to a smartphone?
- How many smartphones are in your household today?

That's not just change. That's *fast* change.

A primary reason that managing kids online is hard is simply this: “Kids Online” itself is a brand-spanking-new reality, bringing with it a whole list of shiny-new problems.

The basic responsibilities and blessings of parenting have not changed (more on that later); but the particular challenges of this issue haven't already been overcome and documented by generations before us. We are all, to a degree, [flying by the seat of our pants](#).



But don't lose hope, and don't lose confidence! You are the parent, you are in charge, and you *can* figure this out.

The simple steps outlined in this report will help you get started doing just that.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

## 1. Limit (or STOP) Sharenting

- Sharenting is sharing pictures & information about your kids in public online places.
- Don't do it.
- When you do share a photo or information about your kids, share it with friends only, not with the general public.
- Don't use hashtags such as #babybathtime or #naptime which make it ridiculously easy for the bad guys to find photos of your kids. The world is not full of nice people.

When you post information or pictures of your kids online—on social media platforms, your blog, or wherever— it's there for everyone to see. *Forever*. Other people can then easily find it and use it for their own purposes.

This is not always done maliciously. Perhaps a busy marketing intern finds your child's photo incorrectly included in a set of free images and doesn't properly vet it to verify that her company can use it. She just grabs it and slaps it next to the product she's trying to sell.

However, the intent of the person using your kids' information or photos is beside the point: the damage they can do is incalculable. Both bad guys and well-intentioned people can misuse your kids' data and pictures . . . so, don't overshare it!

[Click here to read how one child's stolen photo](#) was misused. Thankfully, after a difficult battle, the company which had illegally used that girl's picture settled with the mom. But that settlement didn't erase what had happened.

## 2. Lock Down the Privacy on *Your* Social Media Accounts

Yes, I am still talking about the parents here.

If you want to protect your kids, you must maximize the security settings of any social media that *you* use. Bad guys want information *about you and about your kids*. Don't make it easy for them to get that information.



[Click here for a checklist to improve the security settings on your facebook account.](#) But don't stop with facebook—whatever social media platform you use, go to its settings and lock it down.

Verify that people tagged as your friends *actually are* your friends. If you've not done this in a while, set a task to check through 10-20 people on your Friend-list once a week until you've gotten through the whole list. Unfriend any account that looks inactive or that is for someone you don't know.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

Be slow to accept a friend request from someone you've not seen in ages. *Bad guys have become very adept at pretending to be an old friend*—fake pages are created every day. If you aren't sure whether a friend invitation is legitimate, ignore it or delete it.

For the inside-scoop on how hackers use social media as a tool for evil schemes, check out this [4 minute story by Cisco](#). Here's the summary:

The video opens with a smart, 20-something hacker with red hair and pig tails. Your incorrect assumption that all hackers are cave-dwellers across the ocean is about to get dissolved. We watch her snooping around a CEO's Facebook page, where she easily figures out the name of his wife. Then the hacker looks around the wife's Facebook page, until she has enough data to send the wife (a busy young mom) a friend request, seasoned with a tidbit about where the wife attended college. The mom accepts the friend request, enabling the hacker to see not just public posts but posts "for friends only."

This story ends with a ransomware attack on a business (By the way, if you are a business owner scared about ransomware, good for you, you should be scared. [Contact us](#) to learn about protections). But the same strategy modeled in this story, using social media to research and eventually access needed information, is used by other types of hackers as well: pedophiles, kidnapers, and other ilk. In fact, we unknowingly make it way too easy for them to get the information on the kids they want:

Because we share a ton of information—pictures, videos, etc—hackers can easily stalk a child virtually, learning the child's location through a parent's posts. Parents proudly post pictures with captions that may disclose geographical locations. Or, the picture may include features which Google Street could identify, such as a local park or even perhaps the front of their house. If the kids in a picture are in sports, they may be wearing a jersey identifying where they go to school. The metadata in pictures can sometimes have GPS location tags as well.

Careless oversight is often a factor unnecessarily placing children at risk. Here's an example of that: my company was hired to do a cybersecurity assessment for a school district as they were responding to a data breach. It was rather easy to find the students without breaking in, as some of the teachers were actually posting class pictures for all the world to see— on Twitter of all places!

Social media is also a great place (from the hacker's perspective) to infect a computer through a malicious picture. Hackers send a slightly blurry picture to their target with the quick question, "Are you in this picture?" When the target clicks to open the picture, the hacker gains access to the family computer.

—[Nick Espinosa](#)

Disclaimer: *Locking down your privacy settings on Facebook or any other social media platform is not an automatic guarantee that your account is secure. Yes, it is more secure than if you hadn't maximized your security settings. But—for Facebook especially—there's no way*

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

to make it “very secure.” Facebook *says* they are committed to security, but their frequent fumbles belie the truth. Here are two examples:

- [133 million phone numbers of US Facebook users exposed](#)
- [Strangers let into Messenger Kids chats due to “technical error”](#)

These are only the biggest two stories of early September 2019. The phrase, “another day, another Facebook breach” is not much of an exaggeration. See #1 for how to handle this reality.

### 3. You Own the Devices, You’re in Charge: Make that Clear

All the parenting books on the planet (that are worth more than bird-cage liner) agree with this: you are the one in charge. You are the adult; therefore, you get to set the policies and be the leader.

That is not permission to be overly bossy. Rather, it’s a recognition that *sometimes your kids will see you as a meanie* even when you are just doing your job. You’ll be happier if you own up to this fact: your kids’ perception that your rules are unfair comes from a *childish* perspective.

Technology discussions are easier to manage without the child saying “But it’s mine.” So, we recommend you own all devices from the beginning, simply to make this conversation easier on you.

As the adult in charge, you must teach your kids *digital hygiene*. Andrew Yao, co-founder of [Safe Lagoon](#), explains digital hygiene this way:

You wear a seatbelt when you get in the car. You put anti-virus on your computer. Similarly, your kids need to understand, from the first time they start using a smartphone, that there is a parental monitoring tool in place. It’s just the way things work.

At Safe Lagoon, we don’t take the “spyware” approach that some tools do. We don’t hide from your kids that you are monitoring them. We *want* your kids to know that you are using Safe Lagoon, because we see our software primarily as a tool that is only effective when parents use it in conversations.

“Mom, can you extend my screentime just 5 minutes so I can finish this conversation with Charla?” or “Son, I see you downloaded a new game, I’d love to see how it works!” are the types of comments that Safe Lagoon makes easy. In this digital age, healthy families must be having such conversations *every day*.

**What if it’s too late for that?** What if your teenager bought his device with his own hard-earned money? Or, what if you’ve been sitting on the sidelines for years, letting your teenager “sail free,” but now you want to step in and be the director of his digital world?

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

Two key principles address this difficult situation:

- **Get your own mindset right.** You still have primary ownership of your child's device, even if he paid for it, because you provide what's needed to make it work. Does your child or teenager pay for electricity, Wi-Fi, or internet at your home? No? Doesn't even pay his portion of the monthly phone bill? Then you *actually are* the boss of his gadget. *Get that clear in your head, even if it's not clear in your child's thinking, and you'll be more effective.*
- **Get help.** Now that your mindset is clear, **you need help.** *If you've been letting your teenager roam free digitally for years (or even months/days), you cannot just grab the reins, yank, and expect compliance.* The journey from "roaming free digitally" toward respecting your authority in the digital world is complicated to navigate, and different for each parent/child relationship.

Regarding the need to get help, maybe you are thinking either:

"Are you sure I can't just figure this out on my own? I know how to take away my kid's stuff or ground him. I can administer negative consequences for this just like I have for a hundred other parenting issues."

Or even simply:

"OK, I need help, but where do I find it? How do I even start to look?"

In response to both thoughts, I'd like to quote something my dad, Nick Grabar, taught me:

**Often in life, our problem is not that we have the wrong answers.  
Our problem is that we are not asking the right questions.**

**Here is my first stab at asking the right questions in this situation:**

- If you have decided to be more involved in your child/teen's digital life, but you haven't been too involved so far, how do you exert that parental authority effectively? In a way that minimizes the chance your child will simply run away and maximizes the likelihood they'll listen to you?
- If you have never looked at the private messages or pictures on your child's smartphone, what's the process and attitude you should use to
  - improve the likelihood that they will "let you in" thankfully (or at least willingly) and
  - decrease the likelihood that they will pitch a fit and stomp away, telling you to never even THINK of getting their phone's password from them?
- How does your desire to oversee your child's digital communications and online activities sync with the complexity of your relationship with him? A relationship which is highly affected by your unique personality, his unique personality, and the

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

myriad relational habits (both good and bad) you have both formed from years of interacting with one another?

Those are profound questions, yet you don't need cyber-gurus to help you answer them. Yes, you *do* need some tech savvy tools (see #5) and protections (see many other points in this paper), but for *these fundamental questions just mentioned*, high technical skills are not required. So, where do you begin to find answers?

Start by seeking guidance from **local** resources. You can't learn great parenting from reading a book or a whitepaper—yes, these things can *help*, but ultimately *you need face-to-face conversations and relationships to help you and your child get through this*. Here are some good places to start:

- Your pediatrician
- Your local mental health agency
- A licensed therapist
- A local crisis center or local Children's Advocacy center
- Notice families that seem to have good digital hygiene, at your church, gym, or library, and ask them for advice. Nothing beats good, old-fashioned, one-on-one conversations.

Also, but secondarily, here are online resources to help your family navigate this journey toward more parental involvement in technology management:

- Missingkids.org has an easy-to-navigate website packed with resources. Start by [choosing a short video from this page](#). Videos are tagged by age and by topic, so it's easy to find what you need. Watch a video *with* your child, then *discuss it* with him.
- BSA has an excellent one-page explanation of how each adjective in the Scout Law ("A scout is trustworthy, loyal, helpful, friendly, etc.) applies to online communication. [Print it out here](#), and tack it to your fridge.
- Ruth Grunstra has an outstanding stack of blog articles addressing the challenges and complexities of parenting. Skim down the list of [categories on the right side of this page](#) to find a topic of interest. I met Ruth 13 years ago. At least half of the parenting skills I have acquired or honed since then have been through observing and modeling the way she parents her kids. I am delighted that she started this blog several years ago, as her youngest started to fly the nest, and I commend her insights to you.
- Focus on the Family has some [great resources here](#), in an easy-to-navigate arrangement of topics.

It's normal to feel like pulling your hair out sometimes. Parenting is not for the faint of heart. Don't give up. Keep looking for the help you need. Your kids are worth it.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.



This paper is a free resource. Further distribution is permitted if this footer is retained and the contents are unedited. [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids) [www.linkedin.com/in/alisonmeredith7/](https://www.linkedin.com/in/alisonmeredith7/) Page 9 of 28

## 4. Be “Over The Shoulder” (OTS or MOS or POS) Often

If you walk up to your child’s back while he is typing on his smartphone, you may see that he just typed “OTS” in one of his chat conversations. Translation: your child is telling his buddies, “An adult is now *Over The Shoulder*, so we need to alter our conversation.” Everyone in the chat immediately dampens what they are saying.

If this happens, just confidently say something like this:

“Hey there! Oh, *OTS*— I know what that means, and you are *right!* I am *definitely* over your shoulder. What’s the news? Oh, chatting with Cathy? Great, how’s she doing today?”

This is your opportunity to be a goofy parent so *play it up*. You didn’t sign up for parenting because you wanted your kids to always think you are cool. They want and need to know that you are interested in their life, even when they act unhappy about your persistent interest.

Here’s the hard truth: *OTS* is still the best tool in your toolbox to keep your kids safe online. This doesn’t mean you are a hovering, helicopter parent. This doesn’t mean you have a new full-time job of standing behind your kids all day long. It simply means that you are frequently glancing at their online behavior and their digital communication, so that your kids are accustomed to your involvement.

Note: “*MOS*” and “*POS*” are growing in usage and convey the same idea: **Mom Over the Shoulder** or **Parent Over the Shoulder**. Crib sheets on current texting acronyms can be found [here](#), [here](#), and [here](#).

A corollary to “Being *OTS*” is this: *Require that your kids’ screentime occurs in public places in the household, places where other family members will frequently pass by and observe the screen.*

## 5. Use Tools to Monitor & Manage Your Kids’ Digital & Online Activity

*You can’t do this alone!* *OTS* (see #4) is essential but not sufficient. You need a tool to help you, and we have two great ones to recommend:

- [Securly](#) was developed specifically for Chromebooks.
  - *If your child or teen uses a Chromebook, we advise you to use Securly.*
  - Read more about it here: <https://www.securly.com/>
- [Safe Lagoon](#) is our top-recommended parental control app.
  - *If your child or teenager has a smartphone, we advise you to use [Safe Lagoon](#).*
  - It is a comprehensive and intelligent solution which automatically alerts parents to potential issues. Some of its many features include:

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

- Easy-to-read daily reports listing which websites your kids have visited, which friends have captured their chatting attention, and how long they've spent on various apps.
- Easy-to-configure schedules, allowing parents to set limits on games and internet access.
- Information to help you spot possible cyberbullying
- [Here's a detailed video review](#) explaining why one mom loves the features, flexibility, and pricing of this product.
- You can get a free trial by [clicking here](#).
- If you get Safe Lagoon (or any monitoring tool), sit with your child while you are configuring it.
  - Discuss how you are setting it up, and why.
  - Explain to your child what digital hygiene is (see block quote on p. 7) and why it's important.
  - For Safe Lagoon, this configuration takes 20-60 minutes, and you'll need both your phone and your child's phone.
  - Start the conversation by asking your child *open-ended questions*, such as “Tell me what you think about spending time playing games on your phone,” instead of closed, specific questions such as “How long do you think I should let you play Angry Birds per day?”
    - You may get to those specific questions *later* in the conversation, but *start* with the open ended ones. Give your child a chance to open up and tell you his thoughts. Once he knows that you've given him your attention and heard his thoughts, he'll be more likely to listen to your insights.
  - When I did this together with one of my sons, the configuration took longer than I expected but was *time well spent*—because we spent that time discussing why I wanted to install Safe Lagoon, what it could do to improve safety, and how it could enhance our communication.
    - I asked my son for his input as we configured his phone, and was pleasantly surprised that he had *a lot* to say. What I thought might become a parenting battle instead turned into a lengthy and delightful time of listening to my son and hearing his perspective on digital communication.

**Tools are NOT a “set it and forget it” solution.** Andrew Yao, co-founder of [Safe Lagoon](#), says it this way:

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

All of us on the Safe Lagoon team are parents, first and foremost. We created this app out of our own desire for more intelligent data about what our kids are doing online. But we have always seen our app—and will continue to perceive it this way—as only a tool. Any tool must be picked up and used properly to be effective.

To use our tool, you just need to communicate with your child. We give you the data, in an easy-to-skim format. You simply pick up that data and incorporate it into your conversations. Talk to your kids about what they are doing online and in their digital communication. Who are their friends? Ask them. Ask them about the apps they are using—“How does Snapchat work? How does this app or that app work?” You must maintain open lines of communication for Safe Lagoon or any such tool to be of value.

—Andrew Yao, Co-Founder, [Safe Lagoon](#)

**The monitoring tools that come free with smartphones are not enough.** These default parental controls allow you to block apps based on their classification. So, for example, you could indicate that your child is only allowed to download apps which are “suitable for ages 6 and up.”



Here’s the catch: **there is currently no regulation on how apps are classified. App Developers simply announce the appropriate age-range of their app.** A University of California student, for example, [was selling drugs through an app that was marked as appropriate for “Ages 4+”](#)—screenshot pictured at left. See that “4+” in the lower right-hand corner? The default monitoring tools on

smartphones everywhere saw it too, and gave it a quick “A-OK” rating.

So, let’s get this straight: if an app developer wants to create an app that enables people to easily buy drugs, and wants to especially target teenagers, what does he do? Well, one key is to make it look super-safe at a glance. He gives his app the tag “safe for ages 4+” so that most parents glancing at it will just gloss over it.

The previous two paragraphs, and the following paragraph, are adapted from explanations given by Lisa Good, author of [Are Your Kids Naked Online](#).

## 6. Look for Hidden Apps or Dark Apps

A dark app is a hidden vault where pictures and other information can be stored. If you are walking toward your child and he quickly flips his phone over or shakes it, he may be using the “emergency shut down” feature of one of these dark apps.

*When you are looking through your kid’s phone (it’s your device—see #3—so of course you have the password), check to see if they have any duplicates:*

- Two navigation apps?
- Two calculator apps?
- Two music apps?

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

Such redundancy may mean that one of them is a masquerade. Lisa Good, author of [Are Your Kids Naked Online](#), explains:

For example, a parent might click around a navigation app and find that it works fine to give directions. The parent doesn't give it another thought. But the teenager knows the secret password to get into that app. That app's "face," navigation, is masquerading its real purpose: a vault to store pictures and information that he doesn't want others to be able to see.

Go to the Google Play or Apple Store on your child's phone and search for "Hidden Apps" or "Vault Apps" or "Hide Photos." If such searches reveal something already installed on your child's phone, you need to have a conversation with him. This is not a foolproof way to search for Dark Apps, as they keep appearing and disappearing, but it's an easy way to start.

## 7. Teach Them How to Interact Online

Kids are *kids*. They don't know how to behave. They need to be taught self-control and good manners.

That's obvious to us in real face-to-face interactions, but we forget that they need the same lessons about online behavior. Start your conversation with these bullet points. Pick up the conversation weekly or more often, using examples from actual online posts that you or your child have read.

- Whatever you post online will be there forever. So, think twice before posting anything. Think about your future boss, who will be searching your online presence before offering you a job.
- Social media is a terrible place to have heated arguments. Having an informed opinion is important. Learning to defend that opinion passionately, reasonably, and respectfully is fantastic. However, putting all that passion, reason, and respect into a digital or online conversation just doesn't work. Save it for face-to-face conversations over our dinner table, or join a debate team.
- Don't accept friend requests from anyone whom you don't actually know as a face-to-face friend.
- People say mean things online which they are not brave enough to say in person. If you respond to them, you give strength and value to what they said. So, ignore them.
- When you see someone being bullied online or in person, don't stay quiet. Always report what you observe to the adults in charge.

- Cyberbullying is a complex, far-reaching, and growing problem. The limited scope of this paper does not allow space to even begin to explain it. To learn more about this crisis and how to respond to it, consult anything created by [Dr. Sameer Hinduja](#).
- For a more comprehensive list of topics to discuss with your kids:
  - [Are Your Kids Naked Online](#), by Chris Good & Lisa Good
    - Buy it, read it, keep it on your shelf, and use it often as a resource.
    - Every chapter ends with a “What You can Do” bullet list, including many suggested conversation-starters.
  - [Questions Parents Should Ask Their Children About Technology](#), by Sameer Hinduja and Justin Patchin
    - Free downloadable PDF
  - Sexting is a crisis in teen culture. This paper does not have space to fully explore this issue, but here are a couple of great resources to get you started:
    - [In this article](#), Kyle Roberts defines sexting and gives tips on how to discuss it with your tweens and teens.
    - [In this article](#), BJ Foster writes a wake-up call to parents and then offers advice about your tone of voice, your manner of questioning, and things you can discuss with your teens regarding this sensitive and important issue.

## 8. Delay Social Media as Long as Possible

Kids don’t need social media. It’s hard to let them be on it “a little bit,” so consider not having them on it at all. To see family updates, they can look over your shoulder onto your accounts. To keep up with friends, encourage them to be old-fashioned and have actual play dates.

As teenagers get older, let them get their feet wet in managing their own accounts. But even then, remember that teenagers still need lots of guidance here—*especially* when they insist that they don’t.

*What is **this** suggestion doing in a white paper purporting to give tips for keeping kids safe online?* Just this: The psychological health of our kids responds to social media like the Titanic reacted to the iceberg.

Here’s an article expounding this terrifying reality:

### [Social Media: Society's Titanic](#)

Recently a 16-year girl in Malaysia posted this poll question on Instagram: "Really Important, Help Me Choose D/L." A few hours later she [jumped off a building](#). She chose “D.” At the time of her death the polling showed that 69% of her followers had chosen Death as the

option for her and, suffering from chronic depression, she obliged their choice. At the end of the 24-hour poll, well after her death, the poll ended with 88% voting for Life. The Malaysian authorities have stated that anyone voting for Death was aiding and abetting a suicide and should be held accountable.

This is the world we live in today. Social Media has a pervasive grasp on much of the younger generations and, as we're finding out, that which was once believed to unite us in communication and friendship is devolving into something much worse: an engine for anonymous anger, steep polarization, depression and suicide. Social Media is where civility has gone to die and it's affecting us in ways that only now are we able to quantify after a decade or so of research.

Selena Gomez is a star of film and music with a social media following of over 150 million people (on Instagram alone). At the Cannes Film Festival, she said "For my generation specifically, social media has been terrible, I understand that it's amazing to use as a platform, but it does scare me when you see how exposed these young girls and boys are. [I think it's dangerous for sure.](#)"

In a comprehensive psychological study performed on children and social media, Jean Twenge uses data from the National Survey on Drug Use and Health to track the mental health and drug use of teens in the United States.

The dataset compiled by the National Survey had responses from more than 200,000 kids between the ages of 12 and 17, as well as over 400,000 responses from young adults aged 18 and older between the years of 2005 and 2017. Twenge found that during this time period major depression symptoms exploded with an astonishing 52% in teens and 63% in young adults [over the past decade](#). 20%, or one in five, girls were now experiencing major depression episodes. Psychological Distress during this time period also rose to 71% in people aged 18 to 25. . . .

No longer do our homes offer a safe haven for those kids who have a hard time with bullying in school. Thanks to the interconnectivity of social media, bullied children now take their tormentors home with them. How would anyone feel if they couldn't escape this, even in a place they typically find security in?

. . . Studies show that people who adopt social media at the age of 19 or older [do not suffer the same rates of depression](#) and mental health issues as their younger peers. Do we need to enable legislation to ensure that no one under the age of 18 can use social media? Do we need to force social media platforms to validate a user's identity and age before allowing a person into the platform? Would that reduce bullying? There is no perfect solution, but we must take steps to reduce the negative effects of social media on today's youth.

If we can't fix this societal Titanic, the iceberg will surely win.

Excerpted from [Nick Espinosa's](#) article at the following link, and used with his permission.  
<https://www.smerconish.com/news/2019/7/10/social-media-societys-titanic>  
Find Nick's videos on his [facebook page](#), and a stack of [his articles here](#).

## 9. Trust but Verify Digital Communications in ALL Relationships—both Peers AND Mentors

Digital communication increases the efficiency, immediacy, and privacy of communication. This is happy, happy news for the sick people whose goal is to abuse our children. Private communication has *always* been a cornerstone of how abusers do their dirty work, so that's not news. The news flash is: WOW, it's so much more convenient, fast, and easy for the bad guys to message our kids privately. People who gain our respect as parents can easily start sending a completely different message to our kids via texting, facebook messaging, or other private communication.

**Wait!** Before you skip the rest of this section, thinking, "Whew, good thing I don't let my kids hang out with *those* types of people," consider this: [90% of child sexual abuse victims know the perpetrator in some way, and 68% are abused by a family member.](#)

EVERY parent has to be vigilant to protect his child from abuse, because every one of us, every day, unbeknownst to us, are running into perpetrators who look just like the rest of us. Hopefully, you will only "run into" such people by passing by them in a shopping center, etc. Hopefully, your family will never experience the trauma of discovering that someone you thought was a friend actually has sick intentions toward your child. But the point is: none of us can know the intentions of another person's heart, so pay attention.

The bad guys who do this type of work are smart; they are in it for the long game. They don't start from nothing and go straight to "I want to see you naked." They start with texting normal stuff, so if we parents are watching the text conversations, we get off our guard. We decide we don't need to check up on texts from that person regularly, because "everything looks just fine."

Then the perpetrator sends a seemingly harmless joke about bathroom behavior—a fart joke, for example. Most any kid would think that funny, of course. This would probably slip past most of us parents, too, think about it: I'm taking a moment from the many other things on my to-do list to glance through my son's phone. I see a fart joke, nothing worse. *In the midst of my busy day*, with everything else on my mind, would I have the clarity of thought to say, "Whoa. Stop right there?" I hope so, but I must say the more likely scenario is this: I'd simply think, "Well, that's immature, but the other stuff this person sends is OK. So, no big deal."

Then they keep up the potty jokes but add some jokes about genitals. *The kid is just a kid and doesn't realize how inappropriate this is.*

This is another reason why OTS and Tools (#4 and #5 above) are both so critical. You need to know who is receiving your child's attention via texts, emails, etc., and *you need to spot-check the messages your child is exchanging with these people.* Your child doesn't have the maturity to recognize when a message thread is getting out of hand, *especially if the messages are from someone whom his family likes and trusts.*

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

Every month or so, I hear something on the radio about a coach or teacher or youth leader convicted of child abuse. Yet I still have the wrong default picture in my head. When I hear “child abuser,” my brain pictures an unshaven man with ragged clothes, grabbing kids off the street. Maybe that happens sometimes, but in fact, many abusers are clean-cut, professional, and trustworthy—correction, they *act* trustworthy, but of course they *actually* are far from it.

- *Often the perpetrators are older youth*, just coming through puberty and wanting to experiment or exert power over younger or smaller kids.
- Other times they are *adults who invest months or years* into grooming kids to become their victims.

To sum: *don't get caught off guard*. Use tools, spot check messages, be vigilant. Also, **require that when teachers, coaches, and other youth leaders text/email/message your kids, you be copied on every such message**. If any of them don't follow this requirement, even for innocuous messages, that is a red flag.

A few places to get more information on this:

- [Know Your APCs](#) is a one-page summary explaining the three things child molesters want and the typical actions they take to gain them. Print it out and give it to the people who work with your children or teens. Give it to your friends and family members who have children. If you work with kids or teens professionally, tack it above your desk and hand it out to the parents of the children whom you serve.
- [Youth Protection Training](#) is a 90-minute online course *free to anyone*—an excellent basic training course on recognizing and preventing abuse. You can split it up into smaller installments, for example 3 half-hour sessions, if you prefer taking it that way.
  - To take advantage of this course, you must create a free [scouting.org](#) account, but you do **not** have to be a registered member of the Boy Scouts of America to take their Youth Protection Training. *Anyone, regardless of whether or not you plan to ever be involved in BSA, can take this course and print the certificate.*
  - **This is a great course for any parent.**
  - **This is excellent training for any church or organization to require of its leaders.** Well-trained leaders who know how to spot red flags are our society's BEST way to combat the crisis of child abuse.
  - I have taken this course; it was eye-opening. Not only did it help me understand how to enact safe policies and vigilance when I am supervising a group of kids or teens, but also *it equipped me to better explain these threats to my own kids.*

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

- This Youth Protection Training class is also appropriate for older teenagers to take. My oldest two sons have taken this course as a requirement of their work as camp counselors. They are therefore very informed about how to protect themselves and others.
- [This link has more statistics about the crisis of child abuse.](#)

## A Personal Story

Recently, I had a personal wake-up call regarding teenagers and digital communications. In early September, as I was finishing this paper, I received a phone call alerting me to group-text conversations involving two of my sons. “No big deal,” I thought to myself, “I’m glad I got this phone call, and certainly need to have a conversation with my sons. But, surely it’s just boys forgetting their manners.”

Wow, was I flat-out wrong.

For starters, I was way behind on the OTS habits I just preached about in #4. So, when I picked up each of my sons’ phones, I observed for the first time text message groups which had started over a month ago. The “conversation” for each texting group was simply swapping memes—sharing laughs with each other. Some were fine. A few were not appropriate. Then there was a large set of memes which were downright ghastly.

A meme is a picture with a caption. Memes are not all in bad taste, but some are.

Here are captions from a few of the many inappropriate memes I found on *my* sons’ phones—I *won’t disgust you by including the pictures that accompanied each of these quotes.* When needed for context, however, I’ll describe the accompanying picture within parentheses.

- “Suck on my secure connection.”
- “Just because it’s criminal to be wicked doesn’t mean it’s wicked to be criminal.”
- “I’m using batcave to torrent porn.”
- “I deadass know how to respond.”
- “Roses are red, nuts are brown, skirts go up, pants go down” (This poem continued for 6 more lines, describing the details of a male orgasm)
- “I just sent a bunch of raunchy memes to my number neighbor, I think I scared him.”
- “You’re the reason nobody likes you.”
- “Menstruation: Wrong place Wrong Time” (Picture of bikini-clad women in the ocean, running toward land away from the sharks in the water)
- “I add brake fluid to my meth so I can stop whenever I want”
- “Jumping off Buildings: How High is Too High” (This phrase was photoshopped onto the title section of a girl’s science fair project poster. The picture was of her standing next to her trifold poster, displaying her research and smiling)

- “Calm down, you’re just a whore who found glasses” (Picture of sexy woman wearing a skimpy shirt with ample cleavage—and wearing glasses, of course)
- “Sorry, I ran out of coal” (Picture of Santa with his pants partly down, sitting on the chimney as if it were a toilet)
- “You turn my software into hardware”

I included this list to shock you, because **we need to be shocked**. *We need to be shocked into realizing how desensitized our young generation has become, and how quickly and easily bad content is thrown at them.* As I talked with both of my sons about this garbage, I learned that they had both seen worse, including the common scenario of a teenager with a [sext](#) on his phone, handing it around to others, showing it off like a trophy.

This story could have been much worse. Here’s what “much worse” can look like—a friend recently told me the following, when I mentioned I was working on this paper:

My son went through a terrible time with this. He got this picture on his phone—a girl sent him a naked picture. He didn’t ask for it or anything, but she just sent it to him, so it was on his phone. He got his phone taken away, went to the principal’s office, there was a whole investigation, he was in big trouble. It was just awful to go through all that and it lasted awhile, it was awful.

He never asked her to send him that naked picture, and he didn’t like it at all. When they investigated it . . . thankfully, when they looked through everything, it was obvious that there was nothing on his phone indicating that he requested that she send that. So, they let him off with just making him do community service hours.

But why did he even have to do that? He didn’t do anything wrong, as I see it. All he did was have a phone, and I guess this girl got his number somehow . . . I don’t know if maybe he or a friend gave her my son’s number—but since when is it doing something wrong to give a girl your phone number?

Anyway, he never would have wanted a picture like that, he was just shocked she sent it and shocked that apparently, she thought he would like it. And I don’t think she got in trouble at all, though I guess I don’t know the details of that. I hope she got counseling or something . . . I think she kind of came from a mixed-up family. In any case, obviously she has issues if she thought that a picture like that would be what my son would want.

Often, less discreet youth send inappropriate content to all their friends. **If your child has a smartphone, he probably has garbage on it that he never requested.** Depending on “how stinky that garbage is,” there could be legal consequences (read more on this [here](#), [here](#), [here](#)).

## Maybe I’m Over-Reacting

I was nearly done writing this whitepaper when I got that phone call (see page 18) which alerted me to look at my own sons’ phones. I assure you that the depth and length of this report changed significantly—hopefully for the better—due to that personal experience. However, *maybe* because the timing of that personal experience aligned so closely with my work on this

whitepaper . . . maybe I'm just highly sensitized. Over-reacting. Too wound-up. Perhaps this is not a cultural crisis, as I am implying.



Besides, let's be real: teenage boys talking about sex is as old as dirt.

OK, I'll cede that point: it's not a news-flash that teenagers (especially boys, but girls too) discuss such things, and often in lewd ways. But there IS a news-flash, and here it is: *this age-old reality has taken a brand-new turn.*

**Teenagers (and often tweens) today are getting this stuff *thrown at them*, whether they ask for it or not,**

**whether they are eagerly seeking it or trying hard to shield their eyes from it.**

- Just a few years ago, teens and tweens had to sneak magazines into dark corners away from chaperones to share such comments and pictures.
- Just a few years ago, the kids who didn't want to participate in such conversations could simply *not go* to the dark corners. It wasn't too hard to come up with a face-saving excuse of why they didn't want to join their buddies in such conversations/places.
- But today, in this digital age, *unless you are raising your kids in a cave* where they have no interaction with other sinful people (sarcasm intended), it's exceedingly difficult for kids trying to do the right thing to "keep their eyes turned away."
- Point in case: every one of the quotes I just listed, plus others, along with the pictures for which those quotes served as captions, were on one or both of my sons' phones. However, *each did nothing voluntarily to put those memes on his phone; he didn't ask to receive any of that.* He received it all because a friend added him to a group text conversation, to which he could not unsubscribe without blocking every number in that group. The group text conversation started out fine, but then went south fast. He could turn off notifications for the group, to stop paying attention to it. But all that garbage was still right there on his phone.
- And, just to be clear: the list I shared on pages 18-19 is *tame*. Many teens and tweens today regularly share digital content *significantly more vulgar* than those examples.

As I was preparing this paper, of course I talked with many people about its contents—my stories and theirs. I was surprised that many *adults* told me various versions of, "This is just the way things are these days; the world has changed. It's just how kids communicate today. I don't particularly like it but . . . what can we do?"

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

Carroll Sue Priddy disagrees with this mindset:

Just because it “happens all the time” doesn’t mean we parents should shrug our shoulders, wonder why “the world has gone downhill”, and act as if nothing can be done.

There is a false philosophy, prominent in every age, that says, “If everyone is doing this (whatever “this” is), then it must be OK for the current generation.” Paul had something to say about such a perspective in Colossians 2:8. He wrote that we should not be taken captive through empty deceit based on human tradition or the elemental forces of this world.

We don’t want worldly-normal for our sons and daughters. We strive for something far better. We as parents need to just *stop* defending inappropriate behavior—stop calling it “normal,” which implies that it is therefore OK. We need to stand up for what is right and decent, and instill in our kids the self-worth to do the same.

Furthermore, we need to *stop griping* about how hard it is to take a stand against lewd, inappropriate, and thoughtless communication, both digital and otherwise. *It has always been hard to stand up for such decency*, in this and every age.

—Carroll Sue Priddy, MS, CEO of [Launched Life](#)  
Launched Life is a program to help 15-25 year olds figure out what their best next steps are toward a successful career path.

## What Do I Do Now?

**First: Figure Out Where You Stand, Ethically and Practically, on Such Issues as:**

- Who is your child / tween / teen allowed to communicate with digitally?
- What topics *are OK* to discuss via digital communication?
- What topics *should not* be discussed digitally, but rather should be addressed via old-fashioned face-to-face conversations and phone calls?
- What content is OK for your child / tween / teen to view and to read?
- [What are your family policies on screentime \(when / where / how long\)?](#) How are these policies enforced?

Until you get these big-picture issues clear in your own head, managing your kids’ digital communication will be difficult at best, and completely ineffective at worst.

And, remember: this is not a one-time problem to solve. These plans need to be re-evaluated as your kids earn freedoms and show responsibility . . . and of course they also need to be altered if your kids don’t respect the rules set in place.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

Lynette D'Avella, mother of four, shares some of her journey in addressing these issues:

A few years ago, one of my sons wanted a machete, to cut grass the old-fashioned way. One of our relatives, hearing of his curiosity, took him to her computer and googled “how to use a machete.” What appeared was an auto-play video, just a few seconds long, of a terrorist beheading someone. She hurriedly tried to figure out where to click “stop,” but he saw the whole thing before she clicked away.

He told me later that day, “Mommy, I didn’t want my eyes to see that.”

“*I didn’t want my eyes to see that.*” Wow, only a child could put it so simply. This has become a catch phrase in our home, and we often turn it into a question: “What do we want our eyes to see?” We talk about how what we see naturally becomes what we think about and talk about, so guarding our eyes is important.

My husband and I have often discussed: Will our kids know the difference between good and evil when they see it on the screen? In this ever “graying” world of relativity, it is essential to install a red-flag mechanism within our children so that when evil appears, they respond appropriately. But how do we do that?

Philippians 4:8 is quite helpful here, directing us to let our minds dwell on whatever is true, honorable, right, pure, lovely, admirable, excellent, and worthy of praise. I talk with my kids about what it means for our “minds to dwell on” something. I explain that we have a choice regarding where we direct our thoughts, and we need to choose wisely. Just because inappropriate content is all around us does not mean that we should remain neutral or apathetic.

Watching family movies provides a perfect context to discuss these issues: why did certain characters do certain things, and why did movie directors choose to show us certain things? Also, it’s helpful to have a family plan covering blanket screen rules, and to teach kids “pre-decisions” of what to do immediately if they view anything inappropriate. Ultimately, parents need to define their family’s ideology and teach this to their kids—so that when we see evil, it will jump out at us and cause us concern.

I certainly haven’t found any shortcuts in this endeavor, though. As far as I can tell, the solution to this issue is simple yet far from easy: Listen to my kids, often. Ask them questions to help them develop their moral framework—prompting them to think about *why* our family takes a stand on certain issues. Listen to their answers. After all that listening, asking, and listening some more, give them guidance.

Let us all be burdened and empowered to respond with truth and wisdom to the challenges facing this young generation.

—Lynette D'Avella

## **Second: Step into Reality. Don’t Live in the Dark**

If you (like me until just a few weeks ago), are still thinking, “Sure, bad stuff is out there, but that just *can’t happen to my kids*, I’ve raised them to avoid that type of stuff,” then consider this insight from BJ Foster:

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.



This paper is a free resource. Further distribution is permitted if this footer is retained and the contents are unedited. [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids) [www.linkedin.com/in/alisonmeredith7/](http://www.linkedin.com/in/alisonmeredith7/) Page 22 of 28

. . . sexting is widespread, and if you've thought, "My son/daughter would never..." I would say that is naive. Any teen is capable, even the ones who seem "pure" and "wholesome." If you have not had a discussion with your kid about teen sexting then start now. If you catch them engaging in it or even if you haven't, prepare yourself for that talk with the following points [\[here's a link to his talking points\]](#).

You may not have raised them to engage in that type of behavior, but again, don't be surprised. Teenagers do not have a core identity yet. They know how to meet the expectations of others, and what face they need to put on that will make others happy. That includes you, but there are many different people whose approval is important to them.

The biggest competitor you have is their peers. When they are home, they show you one face and when they are with their peers, they put on a different one. They aren't being fake or two-faced. The two faces just haven't become one yet. The values you are instilling are not fully a part of them yet.

excerpted from "[You Caught Your Teen Sexting, What Now?](#) by [BJ Foster](#)

If you are just now realizing how bad the content is on your teenagers' phones, *go take a few deep breaths before you talk with them.*

When you do talk with them, stay calm. Do NOT say, "Oh my GOODness are you KIDDING me?" *Go call up another parent first.* Have that type of conversation with *your friends*, then *calmly* go talk with each of your kids, one at a time. *If your kids see how shocked and upset you are, they will be less likely to continue to share with you in the future.*

### **Third: Take a Small Step Toward Helping Your Child Become More Aware**

One of my friends gave excellent advice on how to respond to this desensitization. She sat down next to her son and had the following conversation, holding the phone in her hand next to him, displaying one of the inappropriate memes (he'd already seen it. So, nothing new in showing it to him again). The conversation went something like this:

Mom, calmly: "Look at this." (points to the meme, counts to 5 silently)

Son: (No comment, just sitting and looking)

Mom, calmly: "Think about this." (continues to point to it, counts to 5 silently)

Son: (No comment, just sitting and thinking)

Mom, calmly: "Would your dad or I *ever* post something like this?" (pauses, waits)

Son: (shakes head slowly)

Mom, calmly: "Do you know *any respected adults in our life* who would say or post this?"

Son: (pauses, shakes his head).

Mom, calmly: "Explain to me why this is wrong."

Son: Pauses, then talks—conversation between son and mom continues.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

There were about a dozen people on the text thread I described on p.18-19, and I knew many of the parents of others in the group. So we parents have spent lots of time debriefing, sharing stories, trying to figure out how to handle this. One big shocker is how our own boys don't think this stuff is a big deal. The most common responses they give us are, "It's just 8<sup>th</sup>-grade locker room stuff. No big deal," or, "Yeah, it's bad, but that's the kind of stuff that's out there."

The "aha" our kids need is not just that they shouldn't *post* stuff like that—of course—but also that they must speak up if they are present when such content is shared. Yet, they can't speak up if they don't even notice it, if they are just shrugging their shoulders. *How do we address the de-sensitization of these Digital Natives?*

## Final Thoughts

Digital communication is a new thing for humanity, and in many ways our adaptation of it is not going so well (see [Nick Espinosa's "Titanic" article](#) previously quoted, or [this](#) horrifying [story](#)).

But the core issues related to these new challenges are not a bit new, they've been around for millennia: Parenting is hard work. Good versus evil is still around. Kids need parents to help them learn to navigate the complexities of social interaction.

We who grew up when MTV was "the thing" are Digital Immigrants. This highly-connected, lightning-paced world is still new to us. We didn't grow up with technology, and we are still trying to figure it out. We are the outsiders.

Our kids are Digital Natives. The internet, texting, and all things digital—this is all part of the oxygen they've breathed since birth.

That doesn't mean you're not qualified to guide them through these challenges. Sure, our kids are faster than us at learning any new technology they encounter. But they are *still kids*, and kids still *need parents*.

The challenges we Digital Immigrant parents face are new, yes. We need new tools and strategies, yes. But the fact is that we *don't* need to completely re-invent the wheel when it comes to how to be a parent.

"Good old-fashioned parenting" still works just fine in this digital age. The foundational attitudes and daily tasks that have worked for thousands of years are still the foundation of whatever solutions we implement today: Hug your kids. Look in their eyes for a long moment, smile, and [listen to what they want to tell you](#), without being in a hurry to go do your next thing. Guide them. Remind them that your goal, in everything you do, is to protect them and to provide for them. Ask for their help and insight. Tell them that you love them.

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

## Addendum: Raw Links

The following links were referenced in the preceding pages. **If you are reading this report digitally**, from [www.holstonit.com/protectkids/](http://www.holstonit.com/protectkids/) , then each of the following links has *already* appeared in what you have read, and **this section gives you no new information**. You can get to every one of the following links simply by clicking directly from the report above, as they were referenced.

However, *if you are reading a printed copy of this report*, this section is provided so that you can still find the links by typing in the exact URLs.

### Page 2

[alison@holstonit.com](mailto:alison@holstonit.com)

<https://www.holstonit.com/protectkids/>

[alison@holstonit.com](mailto:alison@holstonit.com)

[www.linkedin.com/in/alisonmeredith7/](http://www.linkedin.com/in/alisonmeredith7/)

<https://www.bristolparenting.com/>

<https://www.facebook.com/HolstonIT/>

<https://www.holstonit.com/blog/>

<https://www.holstonit.com/protectkids/>

### Page 3

<https://amzn.to/2Nr6k4a>

<https://amzn.to/2Nr6k4a>

<https://www.mgma.com/>

<https://www.holstonit.com/about-us/lego/startateam/>

<https://fpcjc.org>

<https://www.facebook.com/BSATroop3Admin/>

<https://www.holstonit.com/services/network-services-computer-support-it-consulting/>

<https://www.holstonit.com/comit/>

<https://www.holstonit.com/services/email-spam-protection/>

<https://www.holstonit.com/services/data-backup-recovery-business-continuity/>

<https://www.holstonit.com/services/virtualization/>

<https://www.holstonit.com/services/hipaa/>

<https://www.holstonit.com/our-clients/>

<https://www.holstonit.com/awards/>

### Why Is This So Hard? page 4

<https://www.wonderopolis.org/wonder/can-you-fly-by-the-seat-of-your-pants/>

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.



This paper is a free resource. Further distribution is permitted if this footer is retained and the contents are unedited. [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids) [www.linkedin.com/in/alisonmeredith7/](http://www.linkedin.com/in/alisonmeredith7/) Page 25 of 28

## 1. Limit (or STOP) Sharenting page 5

<https://soheresus.com/2015/06/12/down-syndrome-genoma-copyright-infringement/>

## 2. Lock Down the Privacy on *Your* Social Media Accounts p. 5-7

<https://www.holstonit.com/2019/09/05/improve-your-facebook-security-use-this-checklist/>

<https://www.youtube.com/watch?v=4gR562GW7TI&t=95s>

<https://www.holstonit.com/about-us/contact-us/>

<https://www.linkedin.com/in/nickespinosa/>

<https://nakedsecurity.sophos.com/2019/09/06/database-exposed-133-million-us-facebook-users-phone-numbers/>

<https://nakedsecurity.sophos.com/2019/08/30/facebook-technical-error-let-strangers-into-messenger-kids-chats/>

## 3. You Own the Devices, You're in Charge: Make that Clear p. 7-9

<https://safelagoon.com/en/>

<https://www.missingkids.org/netsmartz/videos>

[https://filestore.scouting.org/filestore/youthprotection/pdf/100-055\\_WB.pdf](https://filestore.scouting.org/filestore/youthprotection/pdf/100-055_WB.pdf)

<https://www.bristolparenting.com/blog-updatesarticles>

<https://www.focusonthefamily.com/get-help/family-qa/resources/>

## 4. Be “Over The Shoulder” (OTS or MOS or POS) Often page 10

<https://www.usatoday.com/story/tech/columnist/2017/05/21/sneaky-teen-texting-codes-what-they-mean-when-worry/101844248/>

<https://www.verywellfamily.com/the-secret-language-of-teens-100-social-media-acronyms-2609651>

[https://www.webopedia.com/quick\\_ref/textmessageabbreviations.asp](https://www.webopedia.com/quick_ref/textmessageabbreviations.asp)

## 5. Use Tools to Monitor & Manage Digital & Online Activity p. 10-12

<https://www.securly.com/>

<https://www.securly.com/>

<https://safelagoon.com/en/>

<https://safelagoon.com/en/>

<https://www.youtube.com/watch?v=zEnFGSLzvYI&feature=youtu.be>

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

<https://safelagoon.com/en/registration.html>  
<https://safelagoon.com/en/>  
<https://safelagoon.com/en/why-safelagoon.html>

<https://www.usatoday.com/story/news/nation/2019/02/20/california-college-student-charged-creating-iphone-app-sell-drugs/2933182002/>

<https://www.areyourkidsnakedonline.com/>

## **6. Look for Hidden Apps or Dark Apps pages 12-13**

<https://www.amazon.com/Your-Kids-Naked-Online-self-destruction/dp/1732884714/>

## **7. Teach Them How to Interact Online pages 13-14**

<https://hinduja.org/>

<https://www.areyourkidsnakedonline.com/>

<https://cyberbullying.org/questions-parents-should-ask-their-children-about-technology>

<https://educateempowerkids.org/2770-2/>

<https://www.allprodad.com/you-caught-your-teen-sexting-what-now/>

## **8. Delay Social Media as Long as Possible pages 14-15**

<https://www.smerconish.com/news/2019/7/10/social-media-societys-titanic>

<http://news.trust.org/item/20190515091101-3ss0p>

<https://www.theguardian.com/film/2019/may/15/selena-gomez-social-media-instagram-cannes-film-festival>

<https://www.npr.org/sections/health-shots/2019/03/14/703170892/a-rise-in-depression-among-teens-and-young-adults-could-be-linked-to-social-medi>

<https://www.pewinternet.org/2009/11/04/social-isolation-and-new-technology/>

<https://www.linkedin.com/in/nickespinos/>

<https://www.smerconish.com/news/2019/7/10/social-media-societys-titanic>

<https://www.facebook.com/NickAEsp/>

<https://www.smerconish.com/news?author=5c735e4ce79c704c50cb9dbf>

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.

## **9. Trust but Verify Digital Communications in ALL Relationships, both Peers AND Mentors p. 16-18**

<https://www.dosomething.org/us/facts/11-facts-about-child-abuse>

[https://armatus2.praesidiuminc.com/tools/Know\\_Your\\_APCs.pdf](https://armatus2.praesidiuminc.com/tools/Know_Your_APCs.pdf)

<https://www.scouting.org/training/youth-protection/>

<https://americanspcc.org/child-abuse-statistics/>

### **A Personal Story pages 18-19**

<https://www.verywellfamily.com/what-is-sexting-problem-1258921>

<https://kmdlawyers.com/teen-sexting-criminal-charges/>

<https://www.aclu-wa.org/blog/sexting-and-law-press-send-turn-teenagers-registered-sex-offenders>

<https://www.hg.org/legal-articles/sexting-legal-consequences-39370>

### **Maybe I'm Over-Reacting pages 19-21**

<https://www.linkedin.com/in/carroll-sue-priddy-56804726/>

<https://launched.life>

### **What Do I Do Now? pages 21-24**

<https://www.businessinsider.com/screen-time-limits-bill-gates-steve-jobs-red-flag-2017-10>

<https://www.allprodad.com/you-caught-your-teen-sexting-what-now/>

<https://www.allprodad.com/you-caught-your-teen-sexting-what-now/>

<https://www.allprodad.com/contributor/bj-foster/>

### **Final Thoughts page 24**

<https://www.smerconish.com/news/2019/7/10/social-media-societys-titanic>

<https://slate.com/technology/2019/08/maryland-sk-court-case-teen-sexting-child-pornography.html>

[https://www.huffpost.com/entry/teens-child-pornography-sexting\\_n\\_5d6ff6d1e4b09bbc9ef8f108](https://www.huffpost.com/entry/teens-child-pornography-sexting_n_5d6ff6d1e4b09bbc9ef8f108)

<https://www.bristolparenting.com/blog-updatesarticles/be-a-fireplacelisten-to-your-children>

Copyright 2019 by Alison Meredith, who makes no claim or guarantee that implementing these tips will protect anyone.



This paper is a free resource. Further distribution is permitted if this footer is retained and the contents are unedited. [www.holstonit.com/protectkids](http://www.holstonit.com/protectkids) [www.linkedin.com/in/alisonmeredith/](https://www.linkedin.com/in/alisonmeredith/) Page 28 of 28