Distracted living is the greatest challenge for growing up andparenting in the social network. It poses a strain on the personal attention devoted to nurture the parent-child bond. Because the technology seduces us away from being present when we are physically with others, we are not giving one another quality attention. Compounding the multi-tasking lifestyles we lead, is the fact that our children’s childhoods are informing them radically differently than our own. Parents are at risk of being perceived as ignorant or irrelevant as they offer feedback and instruction that does not factor in the reality of the child’s experiences on and off line.

The plethora of apps, over one billion and counting, enable children to access educational routines, games, experiences and communities including texting apps for free and they do not require a phone number assigned by your mobile communications company. Many parents do not realize, for example, that free texting apps, such as Kik and Whatsapp can be downloaded and assign numbers independently from your ISP. Other social media apps that are geared for adult audiences that are popular with youth include: Tinder, ChatRoulette, SnapChat, Vine, and YikYak.

Setting and maintaining age-appropriate boundaries in this web-enabled environment is tricky and achievable. Ultimately the goal is to groom your child to be self-governing and responsible with the cyber-powered applications and tools. Rites of passage typically provide some definitive criteria for conferring roles, responsibilities, rights and privileges and social standing to individuals as they mature in society. It is a way of raising children into adulthood with tangible, meaningful markers openly recognized by the community. Some traditions as examples include baptism, marriage, coming of age (Bat and Bar Mitzvah). The rites of passage for use of cyber devices and apps are presented into five levels (see other side of this document): TinyTot, Early Ranger, Ranger, Early Explorer and Explorer. By the time your child has graduated to Explorer level (age 16) it is as if you are handing over the keys to the car. (Source: A Google World in the Garden of Eden: Five Family-Safe Strategies for Texting and Social Media—2011),

“Parental control” versus self-control

One of the most common temptations of the modern parent is to seek control over the devices and their children. Parental control settings have limited value, more like the training wheels on a bike. Before long the child will master the device and the controls. Parental controls have value as instructive ways to engage and maintain an ongoing dialog with the child about purpose-driven use of the cyber tools.

When the use of parental controls are perceived as training wheels to help the child develop their own self control essential to be secure in the network, the signal conveyed to the child is one of confidence in their ability to become a responsible user. And so the aim of parenting with parental controls is to prepare the child to be in control, and for the parent to monitor in age-appropriate ways.

Today more than ever our children need this “discipline” at early ages. The moral compass communicated with use of parental control settings serves as an internal guidance system, and is the basis for personal security in a cyber-powered world that has the capacity to manipulate and exploit the individual. When our children are expected to make decisions and experience consequences, and given a birth to adjust their thinking and conduct, and then stand corrected; when we exude confidence in their ability to understand why certain behavior is not good for self and others, then it is possible to truly instill discipline.

Note: The word “discipline” is a noun derived from the Latin word “disciplina”, teaching or learning. In Webster’s Dictionary the first definition is “punishment”. The remaining definitions pertain to instruction, self control and a system of rules governing conduct. What type of discipline do you want your child to experience? What discipline do you believe will strengthen your relationship with your child, and help her be secure? (Source: www.bananamoments.com)

See other side for user levels : Tinytot, Early Ranger, Ranger, Early Explorer, Explorer

And be not conformed to this world: but be ye transformed by the renewing of your mind, that ye may prove what is that good, acceptable, and perfect, will of God. Romans 12:2
Cyber Rites of Passage
Setting Age-Appropriate Boundaries for use of devices and apps
(Adapted from: A Google World in the Garden of Eden: Five Family-Safe Strategies for Texting and Social Media)

User Levels

**TinyTot** (2 years and under) The Tiny Tot requires limited to no use of screen time closely monitored. Mostly the interface infants and toddlers require is human and the science on brains reveals that interaction with screens does change the brain. The American Academy of Pediatrics recommends no screen time for children two years and under.

**Early Ranger** (3-5 years) From three to five years of age, the device should be used with strict supervision. The child should not be left alone with the device and passwords are not granted. Applications or games that are permitted for the Early Ranger to use should be logged into the “family approved” app list for User Level 2.

The care giver must be able to see what the child is doing at all times. Kids this age learn passwords by osmosis and are intuitive about figuring out how to access and make applications work. I have heard many stories from parents whose very young children figured out passwords and learned how to access the family centric apps, like Netflix, or the smart phone. These are digital natives. Make no mistake. They do not require training on how to access the tools; rather they require training and supervision on the boundaries for their safe use. So don’t leave them unattended with mobile devices. Ever.

**Ranger** (6-10 years) Children aged six to ten years of age are issued devices much like checking out a library book. They are issued the device (iPad, Notebook, video game) for a designated timeframe, and then returned. There is general oversight. The Rangers should not be left completely alone with the devices. There should be a responsible older user conducting random checks on the applications being used and what is happening on and off line. This is the time to have conversations about the fact that there is NO PRIVACY in the network, and so your child should not be seeking privacy from parents or keeping secrets. Hence, random checks to inspect what you expect: good decisions on the part of your child.

**Junior Explorer** (ages 11-15) At this point, your child has demonstrated that she understands the importance of setting boundaries regarding who has access to her personal information (phone number, address, where attends school, etc.) and knowing the source of the apps being used. The “family approved list” may be expanded to included the new applications that interest your child as a Junior Explorer, and there should be an understanding to seek parental approval before downloading any new app.

Texting: Use of texting must be with the understanding that you will conduct random checks and that all the communications will be “E” for everyone. Drill it into them that there is NO PRIVACY in the net. As with the Ranger, free texting and video chat apps are easily accessed via wireless mobile devices, so be clear with our child about what apps you are approving for her on the family app listing and conduct random checks to verify that your child is successfully honoring the boundaries.

Social media: If it is possible to hold off until your child is 16 years old to create a Facebook, Instagram, Tumblr, or other social media account - that would be ideal. For kids younger than 16, years old check out http://www.YourSphere.com - a kid friendly, digital hang out designed by kids and governed by cyber security experts to ensure that there is security in their social connections and content is appropriate.

**Junior Explorer** (16-18 years) The Explorer user should be ready for social media. At this point, your child appreciates that there is no privacy, that you will be conducting random checks on texts and posts to social media. Periodically review and update the house rules for cyber secure communication with your child - especially if they are pushing for more freedoms. Listen and come up with ways to address their needs that are consistent with your family values. Have your child maintain a list of “approved” apps that she is using and review with you periodically. As with the Junior Explorer user, your Explorer should seek your approval before downloading apps - especially free ones which could contain malware and nefarious influences (including predators). The fact that there is NO PRIVACY in the network is reinforced by random checks to posts and texts. (Source: www.bananamoments.com)

“To educate is to enlighten the mind and warm the heart to the love of God.” — St. Joseph Marello