Supervising Your Child's Use of Technology 101

This tip sheet, current as of May 2010, summarizes the various resources available to parents for monitoring their children's use of the internet, Facebook, cell phones, iTouch/iPhones, and video chatting. Obviously, open communication with your child is the best way of keeping your child safe in his/her use of technology. Outlined below are resources you may find helpful to supplement that conversation.

Internet

The two principal methods of supervising children online are *filtering access* beforehand and *monitoring children's activity* afterward, and many products combine these features to various degrees. For most parents, filtering and modest monitoring software may be enough. Comprehensive monitoring programs are the "big guns" in oversight that you may need in the event of a serious problem, and they can be very elaborate (recording every keystroke entered and thereby recreating everything your child does online and taking periodic timed screenshots of your child's activity).

[1] Filtering and Combination Filtering/Monitoring Software

There are many parental filtering products available, and prices for good products range from $25-40. Typically, a parent-administrator has a password and can pre-select categories to block (e.g., pornography, weapons, violence, intimate apparel, social networking) and/or specific websites. Administrators can opt to be notified via email if children attempt to access objectionable material.

Most of these products include some modest monitoring features, such as lists of websites visited.

- ***Pros***: If set up properly, these products are like an armed fortress, blocking even proxy servers (which really savvy kids may try to use to avoid parental controls).
- ***Cons***: They occasionally overprotect and can be annoying, requiring frequent input of the override password. You will have to experiment over the first week to see what level of sensitivity makes the most sense for you and your family. These programs are not transparent to children, and may give some kids a sense that there's a fun party out there that you're not letting them join. Finally, there's no guarantee your kid won't figure out how to "hack" this software, although PCMag says that the latest version of Net Nanny presents "no hope for hackers."
- ***Well-reviewed Products***: According to www.consumersearch.com, which collects and synthesizes other reviews, and www.pcmag.com, which recently (3/10) reviewed the options, the best currently available filtering and combination filtering/monitoring software products are Net Nanny 6.5, Safe Eyes, and CyberPatrol. One product worth special mention is

OnlineFamily.Norton, a web-based program that is currently free. According to PCMag, the Norton program "rival[s] some non-free parental control systems."

[2] Monitoring Programs

The most comprehensive monitoring programs give you a snapshot of everything your child does online. Thus, they provide both sides of an "IM" conversation, sent and received email, web pages visited (not just website addresses typed), and screenshots of activity. The better programs offer web-based access to the information, so you do not have to go to your child's computer to do your monitoring.

- ***Pros***: You will have a very clear picture of what your child is doing online and will not have any surprises.
- ***Cons***: Your child may have privacy concerns and feel as if you don't trust him/her. In addition, you may find yourself too much in the thick of middle school drama.
- ***Well-reviewed "Big Guns" Products***: WebWatcher ($95.99; no Mac support); PC Pandora ($109) and eBlaster/Spector Pro ($97.95).

[3] Controls Built into Google

Google has a "Safe Search" mode that blocks explicit sexual content. Parents can now lock Safe Search mode, but unfortunately, kids can apparently evade it by clearing their browser's cookies. As a result, this does not seem like a highly reliable method at the moment.

Facebook

There are a few key privacy settings that all parents should know how to activate for their children's accounts. Clearly, anything that a child posts onto Facebook has the potential to circulate widely, because any one of your child's Facebook friends may choose to broadcast a post to an unintended audience. There is *nothing* that you or your child can do to prevent that, and do not let the existence of privacy settings lull you or your child into forgetting this inescapable truth. However, these settings, though imperfect, can help protect your children from encountering random strangers on Facebook and minimize the dissemination of posts and pictures.

Note: Every time Facebook overhauls its system, privacy settings revert to the default of universal access. Therefore, it makes sense to look at the following items every few months.

[1] Keep Strangers from Seeing Your Child's Facebook Profile Page

- ***Why:*** If you do not do this, then Facebook's default of universal access applies, and anyone with a Facebook page can type in your child's name and see all their wall posts and pictures.

Remember, however, that nothing is airtight. At any time, even if you make your child's profile private, one of your child's friends can show the world something that your child posts.

- ***How:***

  At the top right of Facebook home page, click on "Account"

  Click on "Privacy Settings"

  Click on "Profile Information"

  With respect to each item – click "Only Friends." [More on "Photos and Videos of Me" below.]

[2] Restrict Access to Your Child's Contact Information

- ***Why***: Your child has 450 Facebook friends and occasionally, due to a lapse in judgment, befriends random strangers. Here's how to keep your child's email address and cell-phone number, which are frequently displayed on the "Info" page of a child's Facebook profile, private or visible only to certain friends. Again, remember that nothing is airtight and that your child's friends can make this information public.

- ***How:***

  At the top right of Facebook home page, click on "Account"

  Click on "Privacy Settings"

  Click on "Contact Information"

  With respect to each item – mobile phone, current address, IM screen name, enter preferred privacy setting (e.g., "Only Friends," "Only Me," or Customize).

[3] Prevent Strangers from Searching For Your Child's Facebook Profile

Why: This turns off your child's public visibility. Your child's friends can find his/her Facebook page, and you can even set it to allow "friends of friends" to find his/her page, but others (random strangers, college admissions officers, and prospective employers) cannot even see that your child has a page.

How:

At top right of Facebook home page, click on "Account"

Click on "Privacy Settings"

Click on "Search"

For “Facebook Search Results,” enter “Friends of Friends” or “Only Friends”

At the same place, make sure that the box for “Public Search results” is unchecked.

[4] Limit Spread of Embarrassing Photos of Your Child

Why: Claire snaps a picture of Anna at precisely the moment that Anna exercises bad judgment. Claire uploads the picture to her own Facebook page and “tags” Anna in the picture. Immediately, *all* of Anna’s 450 Facebook friends have a “news” item in the Facebook home page feed that shows the picture and says “Anna was tagged in this picture!” By modifying Anna’s settings, you can prevent this news item from popping up and prevent all 450 friends from seeing the picture. Only Anna will see that she was tagged. The tag will be invisible to everyone else. To be clear, the picture will still be on Claire’s Facebook page and will be visible to all of *Claire*’s friends, but there will not be a news item announcing the image to all of Anna’s friends, and Anna will not be identified by name on Claire’s page.

How:

At the top right of Facebook home page, click on “Account”

Click on “Privacy Settings”

Click on “Profile Information”

Find “Photos and Videos of Me”

Go to “Custom” and enter “Only Me”

[5] Block Certain People from Interacting With Your Child on Facebook

Why: Sam is bullying Max and keeps posting very embarrassing items on Max’s wall. Max wants to block Sam from being able to do this and would also like to stop Sam’s harassing messages. One solution is for Max to drop Sam as a Facebook friend. If Max fears the repercussions of doing this, you can just turn off Sam’s ability to interact with Max on Facebook altogether.

How:

At the top right of Facebook home page, click on “Account”

Click on “Privacy Settings”

Click on “Block List”

Enter name of Facebook friend to Block

Cell Phones

Parental controls for cell phones exist, but some seem designed more with wireless company moneymaking, rather than safety, in mind. To avoid any possible conflict with wiretapping laws, this tip sheet only discusses safeguards that you use with your child's permission.

[1] See what your wireless provider offers

Here is a link to a chart that compares cell phone safety features by company: http://filteringfacts.files.wordpress.com/2010/03/parentalcontrolsmobile2010.pdf

AT&T, Verizon, Sprint, and T-Mobile offer features geared toward parents that allow parents to set caps on the number of text messages/downloads per day, to restrict certain numbers, and to restrict what kinds of content a child can access online. These services are available for an additional monthly fee (the range seems to be between $2 and $7 dollars a month). Some carriers also allow you to restrict the time of day that a phone can be used. Verizon and Sprint allow parents to block sending/receiving photos; AT&T and T-Mobile currently do not.

Most carriers also appear to offer a GPS tracking feature for certain phones. Verizon, for example, has a "Chaperone" service ($10/month), and Sprint offers "Family Locator." Some of these features will send parents an email when the child's phone moves outside of a pre-approved zone.

[2] Consider software that monitors texts and cell phone use

Some companies, like *My Mobile Watchdog, Radar*, *Net Nanny Mobile* and *MyKidisSafe*, allow you to monitor your child's incoming and outgoing text messages. These services are primarily geared for "smart phones," like Blackberry, Google Android, Windows Mobile, and iPhone. You download the App, then go through your child's contact list and approve as "safe" an unlimited number of phone numbers. When an unapproved text, email, or call comes through, you are immediately notified and can see any such text or email, as well as your child's response, in real time. Net Nanny Mobile also has a feature that scans all incoming and outgoing texts for offensive/sexual language and sends offending texts to parents.

Note that this type of software is not "spyware." Your child will be aware of this software installed on his/her phone.

[3] Consider a wireless plan crafted specifically for kids

A company called Kajeet markets a phone program designed specifically for 10 to 14 year olds. You buy the phone and choose from among three plans. There is no contract or activation fee. $14.99 currently buys your child unlimited texts and 60 minutes per month. Kajeet comes with free parental controls. You can block certain numbers, specify discrete times that the phone can and cannot be used, and give your child a certain amount of money in his/her "wallet" to spend

on features like ring tones. For an additional $9.99 per month, Kajeet offers a GPS locator for the phone that can enable you either to find a lost phone or, in theory, to track a child carrying a phone.

- ***Pros***: Free parental controls; service runs on Sprint PCS network, so there's nationwide coverage; no contracts.
- ***Cons***: Limited variety of phones; "Kajeet" symbol on home screen may embarrass some kids.

Ipod Touch

Restricting access to inappropriate content on an iTouch or iPhone is a bit tricky, because a determined child will know how to [1] reset all settings, including parent-installed controls and/or [2] use "Hidepod" or "Spy Calc," non-Apple software that disguises impermissible content, typically as a calculator.

[1] Use the iTouch's own controls

You can restrict your child's ability to look at inappropriate content on an iTouch by using its own restrictions. On the home screen, tap Settings>>General>>Restrictions. Next, tap Enable Restrictions and enter a four-digit PIN. This will let you lock the settings and switch several features off. Switching off "Safari" will prevent your child from finding pornography, but it also prevents all other web access, which will likely be unpopular. Fortunately, Apple's App store now has several Safari-like browsers with child-protective content filters. Currently, the best-reviewed content-filtering browser App is *Mobicip*. This costs $4.99 at the App Store and has three different browser settings, elementary school, middle school, and high school. Reviews suggest it is fully functional and comparable in virtually every respect to Safari, minus the objectionable content. To ensure that your child does not download another browser, you should also restrict the "App Store" feature (via Settings Restrictions described above) or, perhaps more simply, keep the password required for purchase a secret from your child.

[2] How to figure out if your child is using "Hidepod"

Hidepod disguises content under a calculator icon. If you do not know the password, it functions exactly like a regular calculator. To figure out whether your child is using this program, go to the Hidepod website – www.hidepod.com/registrationLookup.html – and enter the iTouch serial number, which can be found in two places, on the back of the device and by tapping Settings at the home screen. Hidepod is a fee service, and customers register by device serial number. If your child's serial number is recognized, he/she likely has a Hidepod account.

Video Chatting

In recent years, video chatting sites have proliferated online, and Pyle kids are definitely not strangers to this phenomenon. Most video chatting is benign, but some sites that are rapidly gaining popularity, like Chatroulette, prominently feature video chats with random strangers. The format is that you sign in and random people pop onto your screen. If you do not find them interesting, you click "next" and get a fresh crop of people. In this March 2010 article, http://www.articlesbase.com/culture-articles/chat-roulette-what-parents-need-to-know-2073863.html, the author quickly found material on Chatroulette that was "quite indecent." A recent survey by TechCrunch found that 13 percent of users were either "displaying explicit nudity or appear to be committing a lewd act." Tests of the site by reviewers showed that the average user would be exposed to pornographic material within 2 minutes of signing on.

To get onto Chatroulette, all your child needs is a webcam and an internet connection. There is no registration. Because it is a streaming, p2p network, there is no content control from on high. Although users can "report" bad behavior, a chatter is not banned unless he/she receives 5 such reports, and even then, is banned only for 40 minutes.

Here are steps you can take to reduce/limit your child's exposure to these sites.

[1] Supervise use of webcams

If you have a detachable webcam that plugs into your computer, keep it under your control except when your child is under your supervision. Controlling the webcam will keep your child from showing his/her image online. However, even if your child doesn't have a webcam, she/he can go onto this site and see the images of others.

If you have a built-in webcam, you can disable it altogether through your computer's control panel.

[2] Block access to the sites altogether

- If you have a filtering software product, like Net Nanny or Safe Eyes, you are covered. These products automatically block access to Chatroulette and other such sites and update regularly to block access to new sites as they arise. Note, however, that McAfee currently classifies Chatroulette as "streaming media" and "media sharing" and does not block it.
- You can try to disable it by using your computer's operating system. Source: http://www.ehow.com/how_6042603_block-chat-roulette.html or http://www.technewsdaily.com/how-to-block-chatroulette-on-your-pc-0273/