

## **How to protect your children online whether on a computer or smart phone.**

I know many of us are fearful of our children, especially teens, being exposed to dangers online including cyber bullying, sex texting, and porn, just to name a few dangers, and along with the inherent dangers posed by child predators and pedophiles. As Knights, we stand by the Church in combating such actions which in many cases really constitutes a form of child abuse. I have outlined some tips along with resources that parents should consider in combating this growing threat against our children.

### **Index**

**[Page 1 - Step 1: Decide where your child can and can't browse on the internet](#)**

**[Page 2 - Step 2: Increase your security and privacy.](#)**

**[Page 7 - Step 3: Monitor where your kids go online.](#)**

**[Page 8 - Step 4: Remind kids not to talk to strangers online using these tips.](#)**

**[Page 9 - Step 5: Phone use and etiquette by your children.](#)**

**[Page 10-Step 6: @Nintendo DS Lite, Nintendo DSi, and @Sony PSP issues](#)**

**[Page 12: Additional resources for parents](#)**

### **Step 1. Decide where your child can and can't browse on the Internet *[\(Return to Index\)](#)***

- It's a good idea to visit some sites for kids. Pay particular attention when sites collect personal information.
- Please read the privacy statement and, if you don't agree with it, search a little, to find a similar site that doesn't request personal information. Pay attention to whether the site employs tracking cookies.
- Set clear expectations for responsible online behavior and phone use and consequences for violating those expectations.
- Consider in the beginning, having any internet access be in a shared open space in the house such as a study or living room and not in their bedroom until they have earned your trust.
- Set up a schedule of usage especially on school nights. Also, if needed, unplug the computer.

### ***Block inappropriate content using parental controls.***

One of the best defenses against inappropriate content is to block it before you see it using parental controls. For example, @Microsoft offers a number of its programs

including all operating systems and browsers as well as the Xbox console, with parental controls.

- **Windows Vista Parental Controls.** Windows Vista includes a set of parental control features to help parents monitor, manage, and administer their children's computer use-and help keep them safe.
- **Windows Live Family Safety.** This software helps you filter information based on each child's age. You can also limit searches, block or allow certain Web sites, and monitor what your kids do online. You also have access to guidelines on how to help a child use online communications safely or how to talk to children about inappropriate Web browsing.
- **Xbox parental controls.** Xbox includes parental controls that help you restrict your child's ability to play inappropriate games and watch inappropriate DVD movies.
- **Also check with your ISP to see if they offer parental controls.** Some ISPs such as Verizon offer free parental controls to all of their broadband users.
- **There are downloadable parental control toolbars and programs that are offered by a number of organizations.** I list a number of these at the end of the article.
- **Some routers such as those offered by NETGEAR also offers parental controls as well.**
- **To configure parental controls on Mac OSx systems,** go to <http://theAppleblog.com/2009/01/13/kid-proofing-a-Mac-with-parental-controls/> for further instructions.
- **For more information regarding Microsoft parental controls,** go to: <http://www.Microsoft.com/protect/terms/parentalcontrols.aspx>

## **Step 2: Increase your security and privacy ([Return to Index](#))**

In addition to blocking inappropriate content, it's a good idea to block sites and downloads that might be a risk to your security and privacy. I highly recommend, and this is not a request that you must have a firewall, an antivirus, and antispyware/antimalware software installed on your machine. This also applies to Mac users and Linux users as well. There are quite a number of internet security suites available in the marketplace that combines these programs together as one package, typically, you can find them for free or for a very nominal cost. There are many choices such as NOD32, Kaspersky, Comodo, AVG, Secunia, Panda, BitDefender,

and ®Avast, just to name a few. Make sure you keep these security suites updated as recommended by the manufacturer. Also, you should follow these steps as well.

- **Set limits on downloads.** Free games, free music, animated toolbars, and other downloads can expose your computer to spyware or other unwanted software. Depending on the ages of your children, you can teach them not to download software from unknown sources on the Internet or ask your permission before they download anything. This can help to keep unwanted software off of your computer. It is very important that you also review your firewall logs to see what programs are communicating out and communicating in. Explain to your kids the risks of using peer to peer network software such as LimeWire which can expose your child to unsavory and prying eyes. One thing you can also do is contact the ISP and request content logs of which sites have been accessed. Typically, ISPs now monitor bandwidth use. For example, if your computer is generating over 200 gigs of bandwidth use per month, your account will be flagged by your ISP for excessive use.
- **A child might accidentally infect your computer with spyware or other unwanted software.** Kids might try to download programs from some popular sites without permission. To avoid this, monitor where your kids go online and/or configure your browser to block pop-ups and 3<sup>rd</sup> party cookies. Make sure if you are using ®Windows, especially Vista, the UAC controls are not disabled and make sure IE is in protected mode. Again, it is important to secure your computer as stated earlier in this step.
- **If you are on a Windows machine, make sure you are running Windows update on a daily basis.**
- **Create different user accounts.** ®Windows XP, ®Windows Vista, ®Windows 7 as well as ®Mac OSx allow you to create multiple user accounts for your computer. Each user logs on with a unique profile and his or her desktop. If you are a Windows user, you can give yourself an Administrator account and give your children Limited User accounts. Administrator accounts have full control over the computer. Limited Users cannot change system settings or install new hardware or software, including most games, media players, and chat programs.
- **Adjust Web browser security settings.** You can help protect your child through your web browser. Internet Explorer for example, helps you control your security and privacy preferences by allowing you to assign security levels to Web sites. Other browsers such as ®Mozilla's Firefox and ®Google's Chrome allow you to adjust your security levels in the same manner as well as prevent the browser from accessing restricted sites. Furthermore, if you are using ®IE 8, you can

enable InPrivate Filtering to prevent sites from installing tracking cookies. In Firefox, you can install add-ons or extensions such as NoScript which prevents malicious software from running. Firefox also can be enabled to block 3<sup>rd</sup> party cookies.

- **For those who are technically astute, you can configure your hosts file to block illegal sites.** This is another way to resolve domain names without using the Domain Name System. Almost every operating system that communicates via TCP/IP, the standard of communication on the Internet, has a file called the HOSTS file. This file allows you to create mappings between domain names and IP addresses. The HOSTS file is a text file that contains IP addresses separated by at least one space and then a domain name, with each entry on its own line. For example, imagine that we wanted to make it so that if you typed in www.google.com, instead of going to @Google you would go to www.yahoo.com. In order to do this you would need to find out one of the IP addresses of @Yahoo and map www.google.com to that IP address.
  - For example, one of the IP addresses for Yahoo is 216.109.118.69. If we wanted to map Google to that IP address we would add an entry into our HOSTS file as follows: 216.109.118.69 www.google.com

**NOTE: When inputting entries in the hosts file there must be at least one space between the IP address and the domain name. You should not use any web notations such as \, /, or http://. You can disable a specific entry by putting a # sign in front of it.**

You may be wondering why this would work as we said previously that when you need to resolve a domain name to an IP address the device will use its configured DNS servers. Normally this is true, but on most operating systems the default configuration is that any mappings contained in the Hosts file overrides any information that would be retrieved from a DNS server. In fact, if there is a mapping for a domain name in a hosts file, then your computer will not even bother querying the DNS servers that are authoritative for that domain, but instead read the IP address directly from the HOSTS file. It is also important to note that when you add entries to your HOSTS file they automatically start working. There is no need to reboot or enter another command to start using the entries in the HOSTS file.

- **To learn how to modify your hosts file, click the link that matches your OS.**
  - **Mac users, go here:**  
<http://www.Mactips.org/archives/2007/07/19/modify-hosts-file-change-your-local-dns/>
  - **For XP and Vista users, go here:**  
<http://www.mvps.org/winhelp2002/hosts.htm>

- **Secure your wireless network at home by using encryption.**
  - Wireless network encryption, which encodes the data transmitted between your PC and your wireless router is absolutely essential. Unfortunately, most routers ship with encryption turned off, and many users don't turn it on, leaving themselves completely exposed. If you haven't already, enable your router's encryption, and use the strongest form supported by your network. The Wireless Protected Access (WPA) protocol and more recent WPA2 have supplanted and dethroned the older and less-secure Wireless Encryption Protocol (WEP).
  - Go with WPA or WPA2 if at all possible, since WEP is relatively easy to crack. (You have to use the same form on all devices on your network; you can't mix WEP and WPA.) The keys used by WPA and WPA2 change dynamically, which make them nearly impossible to hack. Use a strong password for your encryption key, such as a combination of letters and numbers of 14 characters or more.
  - If you have an older router that supports WEP only, you'll be safest if you use 128-bit WEP keys--but also check the manufacturer's Web site for a firmware update that will add WPA support. If it doesn't look like an update is likely, consider replacing old adapters and routers with newer models that support WPA. Look for a router that supports the hybrid WPA + WPA2 mode, which lets you use the stronger WPA2 encryption with adapters that support it, while still maintaining compatibility with WPA adapters.
  - Make sure you change the default network name and password on your router. I highly recommend changing the network password on an annual basis. Doing so will make it much more difficult for hackers to commandeer your router.
  - **For instructions on how to enable WPA2 security on your router, go to this informative how to guide by ComputerWorld:**  
[http://www.computerworld.com/s/article/9002706/Tutorial\\_How\\_to\\_set\\_up\\_WPA2\\_on\\_your\\_wireless\\_network](http://www.computerworld.com/s/article/9002706/Tutorial_How_to_set_up_WPA2_on_your_wireless_network)
- **Teach your children to protect their online presence when browsing on a public Wi-Fi hotspot or any unsecured network. Since public hotspots like those found in cafes, malls, and even libraries generally don't use encryption, you should assume that anyone can see your child's Internet traffic unless you take precautions!**
  - Have your children check to make sure it's a legitimate hotspot: Insidious types have been known to set up pirate or rogue routers with familiar SSID names like "wayport", "Veriz0n" or "t-mobile," and then use them to capture unsuspecting users' log-on information and other private data as part of an "Evil Twin" attack. Be extremely wary of these so called "Evil Twin" attacks since a hacker could set up his/her laptop to act as an Access Point, usually it mimics a legitimate hot spot as mentioned earlier. Several commercial and freeware software tools are available that can turn any laptop with a wireless card into a so-called "Soft Access Point". The soft AP will broadcast an identification beacon or Service Set Identifier (SSID) that lets other computers know it is available. This concept is very similar to the

email "phishing" scams, where a message is sent to users tricking them to enter confidential information, such as bank account information or other sensitive username and password combinations. The process of tricking someone to voluntarily provide confidential information has been used for years in a variety of forms; more generally it is known as "social engineering".

- **If your children are using a PC or Windows laptop**, make sure to have them verify that the PC or laptop's software firewall is turned on, and that Windows' file-sharing feature is off; it's off by default in Windows XP with Service Pack 2.
  - To check this setting, open Control Panel and choose *Windows Firewall* (you may have to click *Security Center* first in XP or *Security* in Vista).
  - In XP, select the Exceptions tab, and look in the Programs and Services to make sure "File and Printer Sharing" is unchecked.
  - In Vista, click *Change settings*, then select the Exceptions tab and follow the instructions for XP.
- **For Mac users**
  - Do not share your entire startup disk. Rather, share folders that are necessary or a secondary disk that is dedicated to storage.
  - Encrypt sensitive files using the Encrypt command in the Finder's File menu.
  - When setting privileges, be careful about what you allow guests to access on your computer. If at any time you wish to disable guest access, use these steps:
    1. Open the File Sharing control panel.
    2. Click on the Users & Groups tab.
    3. Click the user "Guest" then click Open.
    4. Choose Sharing from the Show pop-up menu.
    5. Make sure "Allow guests to connect to this computer" is not checked.
- **Make sure you teach your children to never send bank passwords, credit card numbers, confidential e-mail, or other sensitive data unless they are sure they are on a secure site!**

Look for the lock icon in the bottom-right corner of your browser, as well as a URL in the address bar that begins with *https*. Such sites build in their own encryption.
- Don't send sensitive files unless they are encrypted. Again, it is better to be safe than sorry.
- Instruct your children to watch for anyone who might be staring or spying on their activities on the computer. This is common sense. If your children suspect someone is viewing their online activities, advise your children to move away. Advise your children to notify an authority figure nearby immediately if they are followed by said person.

- **Whatever you do absolutely NEVER EVER save your log-on information, especially if you are using a public computer such as in a library. That means avoid clicking the box that says Save My Password or Remember Me. This will allow the next user of this machine to possibly log on to this web site as you. And we do not want that! Find and click the “log out” button before you leave if you are using a public computer!**
- Erase your web browsing history and restart the computer (if you can't log-off).
- **If your child is using a public PC, consider having the child scan the machine for viruses using ClamWin installed on a USB drive, preferably, one that can be encrypted with a password.**
- Disable Wi-Fi Ad-hoc Mode – Disabling this in your Wi-Fi settings will prevent your machine from connecting to someone's computer that you don't know. Most normal Wi-Fi connections use Infrastructure mode, where as Ad-hoc meshes a group of Wi-Fi users into a pseudo network. To learn how to disable Wi-Fi Ad-hoc mode, follow the steps on this article:  
<http://mobileoffice.about.com/od/mobilesecurity/ss/disableadhoc1.htm>
- Always turn your Wi-Fi off when you're not at a hotspot. Most laptops and netbooks have a button for activating and deactivating the Wi-Fi antennae. Hackers can use your Wi-Fi radio or antennae to create peer-to-peer Wi-Fi connections with your computer and access it directly.
- For better security, consider signing up for a paid subscription to a hotspot network such as @Boingo or @T-Mobile. Both companies provide connection software that encrypts your sessions automatically.
- Another way to secure a public wireless link is by using a virtual private network, or VPN. VPNs keep your communications safe by creating secure "tunnels" through which your encrypted data travels. Many companies provide VPN service to their mobile and offsite workers, so check with your IT department for connection instructions.
- You can try also using a paid service such as Boingo's Personal VPN (free trial with Boingo subscription, \$30 to keep), @JiWire Hotspot Helper (10-day free trial, \$25 per year) or @Witopia personalVPN (\$40 per year). All three of the services are simple to install and use.
- Finally, if you don't mind connecting through your home or office PC, you can log in to a public hotspot securely by using such remote-access programs as @LogMeIn or @GoToMyPC.

### **Step 3: Monitor where your kids go online ([Return to Index](#))**

- Keep computers in easily viewable places, such as the family room or kitchen.
- It might not be possible to be present whenever your children are online, but it is possible to check later to see where your children have spent their time online.

- For example, if you are using Internet Explorer, you can review where your children have visited by reviewing the History list and see all the places your children visited online. To view your Internet History, click the History button on the IE toolbar. Most other browsers have similar features.
- Check your firewall logs.
- Many parental control programs can provide content and URL logs pertaining to your children's browsing history.
- In extreme cases, you could install keylogger software which allows you to record what your children have entered on the computer and monitor their activities without their explicit knowledge. There are a number of programs available on the marketplace such as [@REFOG Keylogger](#). **Again, this is only as a last resort! I urge parents to talk with their children first if you have concerns about their online activities and work with them before resorting to this method!**

**Step 4: Remind kids not to talk to strangers online ([Return to Index](#))**

Real-time chats, social networking, and instant messaging can be a great way for children to discuss their interests and build friendships. But the anonymity of the Internet can also put children at risk of falling victim to imposters and predators. To help minimize your children's vulnerability, teach them to take precautions such as:

- Use only a first name or nickname to identify themselves.
- Never disclose a phone number or address.
- **Never send photographs of themselves and definitely advise your children against video chatting!**
- **Never agree to meet someone they met online without supervision!**
- To help protect your children from being contacted by strangers while instant messaging, configure your software to allow only approved contacts.
- Talk regularly with your children about the online activities in which they are involved and Internet etiquette in general. Children should know the rule that many adults have learned from painful experience: Do not say online what you would not say in person.
- **If your child frequents social networking sites such as @MySpace, @Twitter, or @My Facebook, it is critical they learn how to properly configure their accounts. This excellent article by PC World is a good primer to learning to**

**avert disaster and provides a good object lesson for your children.**

[http://www.pcworld.com/article/167057/how\\_to\\_avoid\\_facebook\\_and\\_twitter\\_disasters.html](http://www.pcworld.com/article/167057/how_to_avoid_facebook_and_twitter_disasters.html)

- Encourage children to be self-protective. Remind them that anything they say on the Internet or in phone text messages can be shared with others and misused. Ask them to consider if they want what they are saying and doing broadly disseminated. If not, they probably should not say or post it. Emphasize that this could affect their ability to go to college or get a job! Employers and prospective schools now troll the internet for any information concerning a candidate and right or wrong, if that information is on the internet, it is open game!
- Be specific about the risks of cyber-bullying and their need to tell you if something that bothers them occurs. Cyber-bullying is wrong and should be reported immediately!
- Respect for adolescents' privacy is important, but tell children that you may review their online communications if you have reason for concern. Here it is important that parents build trust with their children but also extol that this is a two way street, they need to give you respect and follow the rules if they want your trust.
- Explain that sex texting is wrong, dangerous, offensive, and disrespectful. Just because somebody else does it, doesn't make it right or appropriate! Explain that this could irrevocably harm their reputation and their future lives. Furthermore, it could be construed as a criminal act.

#### **Step 5: Phone use and etiquette ([Return to Index](#))**

One of the biggest issues facing our children online, especially those who are teen or tween ages is the proliferation of smart phones like the iPhone and Blackberries. Many of these phones can not only be used for phone calls but can also be used for sending and receiving photos, music, videos, and documents. Many have full featured internet browsers that are accessible on Wi-Fi hotspots as well as the carrier's network. Many allow users to access chat rooms, social networking sites like My Facebook as well as the ability to track each others' whereabouts using the GPS feature.

One of the problems with our society today is that some parents overindulge their children by providing them tools that can have far reaching repercussions if used inappropriately just as if they were using a car or a computer inappropriately.

- As mentioned in step 4, proper etiquette and common sense needs to be impressed upon your children. Children need to be cautious about disclosing personal information.
- You may also want to warn your kids about premium services that can really jack up the phone bill. "Voting" on American Idol and other shows can cost 99 cents or more per opinion and there are some services – such as ring tone downloads - that can cost several dollars
- Thankfully, many cell phone providers today, offer parental controls either as a feature or a downloadable application on the phone. Some offer parental control

services. Unfortunately, many of these services and features are not free. These parental controls can be used to monitor the usage of said phone by your child.

- @AT&T offers some of the most comprehensive blocking options. Their Smart Limits program (\*Est. \$5 per month) allows parents to set caps on the number of text messages or downloads per day, as well as restrict when the phone can be used, who can be called or texted, and what kinds of content can be accessed online. (When it was first launched, Smart Limits' blocking was so robust that it prevented return calls from 911 operators; that issue has since been cleared up.) T-Mobile's Family Allowances (\*Est. \$2 per month) and Verizon's "Take Control" plan (\*Est. \$5 per month) offer similar features. @Sprint offers a free service for some phones that lets parents restrict texting and other activities.
- @Radar (\*Est. \$10 per month) is a downloadable parental-control application that has attracted attention. However, it is only compatible with some advanced smart phones, such as Blackberries and phones using the @Windows Mobile operating system, as well as some @Motorola handsets. Radar monitors incoming and outgoing calls, emails, texts and photo messages, notifying parents if contact is made with an unapproved caller (all callers are considered unapproved until their status is changed by parents via the Radar website). Reviewers have been fairly positive about Radar, but say the lack of universal compatibility limits its appeal, especially since it is not compatible with iPhones.
- Just short of blocking your children's ability to kill time with text messages and pictures, parents can at least monitor their whereabouts. The most ambitious of these tracking programs is Verizon's Chaperone (\*Est. \$10 per month per child line), which lets parents monitor the location of their child's phone, either from a home computer or from their own mobile phone. The included Child Zone function lets parents set up specific geographical boundaries; if a child leaves the area, the parent is notified via text message. For the same price, Sprint's Family Locator (\*Est. \$5 per month to track up to four phones) will check on your child's location at specified times and let you see where he or she has been in the course of a day, via maps or text reports.
- There seems to be a naiveté attitude about smart phones. All smart phone users should read this report by Trend Micro: <http://trendmicro.mediaroom.com/index.php?s=43&item=738> . Like your computers, you need to secure your phone!
- **Finally, if you feel your child is not mature enough to handle a Smartphone, don't give them one, especially if you don't understand what features are available on such a phone!**

#### **Step 6: @Nintendo DS Lite, Nintendo DSi, and @Sony PSP issues ([Return to Index](#))**

One other thing I wanted to mention to parents that some of you may not be aware of is that many of the portable gaming systems in use today, specifically the portable gaming systems produced by Nintendo and Sony give children and teens the ability to chat amongst themselves, surf the web as well as utilize the free service known as @Skype. Skype is a VoIP service and application that allows someone to call, chat, or IM someone just by being in a Wi-Fi hotspot or network. What makes Skype dangerous is

that calls, chats, and IMs between users are typically untraceable and are free, unless it is to or from a landline. Furthermore, if the user does not configure Skype properly; it becomes an easy conduit for predators to contact or track your child or teen. It is important to emphasize to your children the need to be careful when using Skype.

**To assure that your children are protected while using Skype, I have listed the following helpful hints.**

**Step 1** Add only friends. When accepting "Add" requests, only authorize people you know personally. You should be able to trust everyone on your contact list.

**Step 2** Be careful with links. Hyperlinks often lead to sites with viruses, adware or scams. Ask for a thorough explanation of each link, even those friends send you.

**Step 3** Exercise caution with the random chat function. Setting your status to "Skype Me" invites anyone—strangers, scammers and friendly random chatters alike—to contact you and view your profile.

**Step 4** Leave personal information off your profile. The public can access anything you enter in your profile. Do not include your email address if you do not want unsolicited emails. Make sure your username does not resemble your real name.

**Step 5** Do not reveal your password or credit card number -- whether via email, chat or call. Even if someone claims to be a Skype employee, do not give it out. Skype will only request your password and credit card number from their secure website. Password security is very important. Make sure to pick something random and hard to guess and use at least one number. Change it frequently.

**Step 6** Buy whatever upgrades and credits you need from the Skype Store.

**Step 7** Adjust your privacy options. Click "Tools," then "Options" and then "Privacy" to control which people can contact you.

**Step 8** Never accept unexpected file transfers.

- There is also an excellent guide to properly supervising your children and teens in terms of selecting and playing video games as well as playing online which is produced by the ESRB which rates video games based on content which parents should read: [http://www.esrb.org/about/news/downloads/ESRB\\_PTA\\_Brochure-web\\_version.pdf](http://www.esrb.org/about/news/downloads/ESRB_PTA_Brochure-web_version.pdf). Furthermore, this guide has other useful resources which I urge parents to peruse in the index listed at the end of the guide.

**\*For Sony PSP users ([Return to Index](#))**

There are some parental controls for the PSP and since it is tightly integrated with the Sony PS3 system, the menu works just like the PS3's, and the settings are in the same place. There are settings for Games, UMD movies, and the system browser very similar to the PS3. It also uses the same password setup, but you set it independently of the PS3's. Hopefully, Sony will continue to add more options for parental controls.

## Instructions for configuring the PSP:

**Step 1** Power on your PSP and then go all the way to the right side of your cross-media bar. Then scroll down to the security settings icon (it looks like a lock and key) and then press "X" to enter the security settings application.

**Step 2** Set a password. Simply select a unique key using the chat input function of the PSP. The password must be longer than four characters. This password will be needed when you start the PSP, the Internet and games.

**Step 3** Set parental controls. Parental controls on the PSP limit the type of UMD (universal media disc) that can be played. This includes both game and movie UMDs. The parental controls use a sliding scale with 1 allowing the most content and 11 being the most restrictive. For more on the PSP's parental controls, see the Resources section for the official PlayStation parental controls manual.  
<http://manuals.playstation.net/document/en/psp/current/settings/parental.html>

**Step 4** Enable the Internet browser start control. Enabling this option limits whether a browser can be started without the password you created in Step 2.

### ***Here are a couple of additional helpful links:***

Sony's Online PS3 Manual Security Settings:

<http://manuals.playstation.net/document/en/ps3/current/settings/security.html#1106>

Sony's Playstation Network Parental Controls:

[http://www.us.playstation.com/content/sites/176/info/frame\\_network.html](http://www.us.playstation.com/content/sites/176/info/frame_network.html)

**\*For Nintendo DS series users (Nintendo DS, DS lite, and DSi) ([Return to Index](#))**

There is some good news in that Nintendo has partnered with @Astaro to provide a filtering service that works with the @Opera browser used on the Nintendo DS series to provide parental controls.

- Follow the instructions on this link to enable content filtering on the Nintendo DS series:  
<http://www.nintendo.com/consumer/systems/dslite/browser.jsp#contentFilter>
- For more info on what Astaro offers: <http://www.astaro.com/ds-content-filter/>
- If your child is using the Nintendo DSi, impress upon them not to use the webcams when communicating on Skype. Parents need to strongly discourage video chatting unless your child is absolutely sure who they are communicating with and the other contact can be seen as well. Otherwise, don't do it!

**I also decided to list some useful resources for parents and again, this is not a substitute for good parenting! ([Return to Index](#))**

**Here is an interesting report that all parents should read titled *Enhancing Child Safety and Online Technologies*:**

[http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF\\_Final\\_Report.pdf](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf)

## **Free internet filtering software choices:**

### **Toolbar choices**

#### **®*Parental Control Bar***

<http://www.parentalcontrolbar.org/>

Download link: [http://download.cnet.com/ParentalControl-Bar/3000-27064\\_4-10539075.html](http://download.cnet.com/ParentalControl-Bar/3000-27064_4-10539075.html)

### **(Free) Full program choices:**

#### **®*K9Protection***

<http://www1.k9webprotection.com/>

Download instructions: <http://www1.k9webprotection.com/getk9/index.php>

#### **®*SafeFamilies WeBlocker for ®Windows XP***

<http://www.safefamilies.org/download.php>

### **For IM protection:**

#### **®*Chat Shield***

<http://www.chatshield.com/>

Download link: <http://www.chatshield.com/download.html>

## **Additional ideas and tools to consider. [\(Return to Index\)](#)**

- If your child or teen does homework using ®Microsoft Office, they should check to make sure any hidden embedded data has been removed that might prove embarrassing. For Office XP and Office 2003 files, your child or teen can download [Microsoft's Remove Hidden Data Tool](#) or if your child or teen is using Office 2007, they can use the [Document Inspector command](#) to view and optionally delete unwanted metadata from their Word, Excel, and PowerPoint files. This also helps to prevent data theft.
- If your child or teen needs to use public computers on a regular basis, consider purchasing a portable USB external drive such as an 8gb or 16gb ®Cruzer and consider running the applications your child or teen uses on that portable drive. Go to <http://portableapps.com/> and consider downloading the myriad of tools and apps available that have been “portabilized” so they can store temporary files, cache files, and history on the portable drive itself.

**Also parents who are using Windows based systems should read how to activate parental controls by going to**

<http://www.Microsoft.com/protect/terms/parentalcontrols.aspx>

**\*For Smartphone users. [\(Return to Index\)](#)**

- A cool app which works for Windows Mobile 5.0 and 6.0 smart phones is @MyMobiler. This allows you to control the phone from your PC and view content on a phone. <http://www.pcworld.com/downloads/file/fid.76385-order,3/description.html>
- Another interesting app for Windows Mobile smart phones is @Windows Mobile Monitor, which will record all SMS messages sent and received, and also the name, time and duration of cell phone calls received. Even calls and SMS messages that are later deleted will be recorded. The software runs silently in the background, but needs to be synched with a desktop application (provided) to get the records of the device.  
<https://www.synergetechsolutions.com/MobileMonitor.aspx>
- Kaspersky offers Mobile Security 8.0 for Windows Mobile and @Symbian OS phones: <http://www.kasperskylab.nl/kms>
- @Mobile-Spy which works on iPhones, Windows Mobile devices and Symbian OS devices allows parents to secretly read SMS text messages and phone details. This is a hybrid app/service: <http://www.mobile-spy.com/>
- **\*For iPhone OS 3.x users**, there is now some vestige of parental controls to prevent your children from downloading questionable apps from the iPhone Apps Store. Just follow the instructions below.

**Step 1** Go to Settings > General > Restrictions on your iPhone.

**Step 2** Tap the "Enable Restrictions" button at the top of the page.

**Step 3** Enter a 4-digit passcode. Make sure it's not something your child can easily guess like a birthday. (It's too bad you can't do letters and numbers since a 4-digit number could easily be cracked by an industrious child with a couple of free hours on their hands.) I really wish @Apple had gone with a stronger password nomenclature. Sigh!

**Step 4** Scroll down to the bottom of the page and choose "Apps." You can set all sorts of restrictions such as blocking Safari or YouTube use, but for this tutorial we're focusing on the App Store.

**Step 5** Tap on an age and a check will appear beside it. The blocked ages will be in red.

On the Apps page you will see settings that correspond to age. Each iPhone App developer is required to assign an age rating to their app and this is where you'll choose a maximum age rating for apps that this iPhone can download. You will notice that currently everything is allowed.

**\*Note:** If your goal is to block the "sexy girl" type apps, 12+ is not enough. You'll have to go down to at least 9+ (you can also block installing apps all together).

**Step 6** Now that the age rating is set, any attempts to download apps with a higher age rating will be blocked. It's important to understand that searches are not blocked. If a search is done for the word "sexy," all the apps are still viewable in the results. However, on the app description page the button to buy/install is grayed out and any pictures previewing the app are not visible.

**Step 7** Hit the "Report a Problem" button at the bottom of the apps description page and let @Apple know what's going on if you find an offensive application that has passed through the ratings system. It even has a choice for "This application is offensive."

**Step 8** Remove the App Store icon all together by switching the "Installing Apps" option to Off on the restrictions page if the age restrictions are not strong enough for you. Then you could choose to just install the apps for your children instead of having them do it.

- For other iPhone and @iPod Touch users, I highly suggest using @Mobicip's **free safe browser**. Here is the link to the instructions for setting it up with parental controls: <http://content.mobicip.com/content/how-setup-parental-controls-iphone-ipod-touch-os-2x-edition> .

Mobicip also offers it for the iPhone 3.x OS as well with instructions located here: <http://content.mobicip.com/content/how-setup-parental-controls-iphone-ipod-touch-os-3x-edition>

- **Finally, parents, before you toss that old phone that you or a family member had been using, I strongly advise that you use its reset codes or menu options to clear the message archives and contacts lists. Furthermore, consider visiting the ReCellular Data Eraser site and learn how to reset that phone and follow the instructions posted. You can also use this on an existing phone if you feel that data might have been compromised or to erase confidential information.**

*The Knights of Columbus believe in strong families and it begins with the parents being involved in their children's lives. When we abdicate our rights as parents*

*we allow others to shape the morals and futures of our children. Technology can be a tool for good or harm so take the time to understand the gifts you give your children.*

*This article was written by Michael Elworth who is the Financial Secretary for Obadiah Council 7642 in Kirkland, Washington. Michael handles security and IT tech issues for our council as well as for his company.*

[\(Return to Index\)](#)