A Family Guide to Internet Safety

“We Guarantee A Safer Internet for Your Children”
Dear Friend,

Thanks for taking the time to read the Children’s Educational Network Family Guide to Internet Safety. My wife and I are parents to five wonderful children who are active users of the internet. I have personally experienced my children stumbling across pornography accidentally and I am (and have been for years) scared stiff by the real possibility that they might be approached by an online predator, be demeaned and threatened by an online bully, or discover sites that promote things like making bombs or anorexia.

After an incident my daughter had searching her name online and coming across pornographic material, and my son discovering how to make a “potato gun”, I knew it was time to take action to keep kids safe from inappropriate content and sexual predators online and began my quest to build a software developing and marketing company that empowers parents to provide children a safe internet platform: Children’s Educational Network.

As our children navigate their way around the Web—finding new game sites, downloading music and communicating with friends through email and instant messaging—I realize it's all about education, staying in touch with what our children are doing and taking the necessary steps to keep them safe as they surf the net.

So whether your concerns are about elementary school-aged children learning to use search engines or managing your high school teen’s growing dependency on a social networking site, we’ll explore the top concerns and issue and give you easy-to-understand tips and guidelines for each topic in our Family Guide to Internet Safety.

We hope that by reading this and knowing more about Internet safety and discovering more about Children’s Educational Network and our parental control TUKI Browser (available in Shrek, Miss America, McGruff The Crime Dog, Loral Langemeier, Noah’s Net themes, and more), you will be happy to join the hundreds of thousands of parents who already think of us as a solution to the dangers of the internet for their kids. We also want you to discover the many benefits of Club TUKI at www.clubTUKI.com.

Thanks again for taking the time to learn about Internet Safety and our incredible software. Please visit www.TUKI.com and you will immediately have access to download and install our TUKI Kid Safe Software.

We look forward to serving you and remember, surf safely!

Greg Writer
Founder & CEO
Children’s Educational Network
# Table of Contents

*Introduction* .................................................................................................................... 3

*2008 Internet Safety Statistics* .......................................................................................... 7

*The Basics* .......................................................................................................................... 9
  - Safe Browsing ................................................................................................................. 9
  - Parental Control Software ............................................................................................ 9
  - Passwords: Get Them and Protect Them ....................................................................... 9
  - The Favorites-Sites Kids Love ...................................................................................... 11

*The Well-Known Risks* ...................................................................................................... 12
  - Porn, Gambling, Racism, Anorexia and hate Sites ......................................................... 12
  - Internet Predators .......................................................................................................... 13
  - Cyberbullying and Cyber Stalking .................................................................................. 13

*The Not-So-Well-Known Risks* .......................................................................................... 15
  - File Sharing, Music and Video Downloads ..................................................................... 15
  - Private Information and Identity Theft ......................................................................... 15
  - Teen Online Privacy ....................................................................................................... 16
  - Email and Instant Messaging ......................................................................................... 16
    - Key Recommendations ............................................................................................... 17
  - Blogging ............................................................................................................................ 17

*The Newest Threats* ............................................................................................................ 19
  - Got Bot? ............................................................................................................................ 19
  - How Do They Do It? .......................................................................................................... 19
  - Signs of Internet Addiction .............................................................................................. 20

*Age Matters* .......................................................................................................................... 23
  - Elementary School Children (ages 5-7) ....................................................................... 23
    - Key Recommendations ............................................................................................... 24
  - Tween Children (ages 8-12) .......................................................................................... 24
    - Key Recommendations ............................................................................................... 25
  - Teens (ages 13-17) .......................................................................................................... 25
    - Key Recommendations ............................................................................................... 26
  - College Bound Teens ...................................................................................................... 26

*3 Simple Rules to Follow* .................................................................................................... 29
  - Parents .............................................................................................................................. 29
  - Kids ................................................................................................................................... 29
  - Remember ....................................................................................................................... 29

*Our Solution* .......................................................................................................................... 30
2008 Internet Safety Stats

• 20% of youth include swear words in their MySpace profiles and 33% of MySpace pages have swear words in the comments sections.

• 18% of youth MySpace pages contain evidence of consumption of alcohol by minors

• 64% of teens post photos or videos of themselves online, while more than half (58%) post info about where they live.

• 32% of all teens and 43% of teens active in social networking have been contacted online by a complete stranger.

• 69% of teens regularly receive personal messages online from people they don’t know and most of them don’t tell a trusted adult about it

• 23% of children have had an encounter with a stranger on the Internet, including 7% of children who reported having met someone in the real world from the Internet

• 79% of sexual solicitation incidents happened to youth while they were using their home computer

• 40% of solicitations began with a solicitor communicating with a youth through an instant message or IM

• 56% of solicitations contained a request for the youth to send photographs of themselves to the solicitor and 27% of solicitations contained a request for the youth to send a sexual picture of themselves

• 34% of youth have encountered unwanted sexual material while online

• Common cyber-bullying behaviors include name-calling, spreading of gossip or sensitive information, threats, teasing, sexual harassment, being ignored or disrespected, and being deceived by a bully who is misrepresenting themselves

• 43% of youth report that they have experienced some form of cyber-bullying in the last year. The incidence of cyber-bullying is most prevalent among 15- and 16-year-olds, particularly among girls.
Our children are our most precious and valuable asset. Our children are also the most vulnerable members of society. Protecting our children against the fear of Internet crime and from becoming victims of such crimes must be a parental, societal, and educational priority. Unfortunately the same advances in computer technology that allow our children to reach out to new sources of knowledge, information and cultural experiences are also leaving them vulnerable to exploitation and harm by computer-sex offenders, bullying. I hope that this guide helps you to begin to understand the complexities of on-line child exploitation.

First, let’s look at some top tips for protecting your family online:

• Keep the computer in a common room
• Establish rules for using the Internet
• Understand social networking
• Help your children keep their personal information protected
• Protect your children’s passwords
• Frequently check your online computer’s Internet history
• Spend time with your children online
• Teach your children cyber ethics
• Be computer savvy
• Teach your children to tell a parent, teacher, or trusted adult if they feel uncomfortable about anything they’ve seen on a computer

Though labels such as “explicit” and “harmful to minors” warn against harmful content, pornography, sexually explicit or violent language or other inappropriate content, much of it still finds its way into our kids lives via their computer screen. In the context of the Web, these concerns have led to the development of scores of blocking and filtering technologies. Sexually explicit material; hate speech; graphic violence including misogynist text and images; content promoting illegal activity, such as bomb-making; obscenity; deceptive and unfair advertising; information about alcohol, tobacco and illegal substances; and offensive language and profanity have been at the core of many discussions about children’s well-being within popular culture. But blocking and filtering technology aren’t perfect. Parents, schools, and even the government via tough laws and penalties, must take an active role in protecting our kids online.
The Basics

Safe Browsing
In recent surveys' parents report their children using the internet at home and at school, almost equally as much. To keep them safe make sure your browser is set to offer built in security and safety features. For example, Microsoft® Internet Explorer (the most popular browser) offers security and privacy settings. Popular search engines such as Google also offer some safety features. For example, Google’s SafeSearch allows you to restrict explicit (sexual) sites and content from appearing in your family’s search results. However, the safest way to offer your kids a fun, educational browsing experience is to get them their very own Kid safe browser.

Parental Control Software
Parental control software, like the TUKI (The Ultimate Kids Internet) Kid Safe Browser, enables you to choose where your child is able to go online, and ensure that they don’t view inappropriate subject matter. Parental controls differ depending on the application offering the feature. Usually there are varying levels so you can customize the program according to the child being protected. For example, for a five-year-old, you would provide a “white list” of pre-selected and parent approved Web sites where you would allow the child to visit. Or you might set up accounts requiring a parent’s login to enable the child to surf the Web, or time limits so your children don’t spend hours on the Web instead of doing homework or chores. You can allow older children or teens more access and flexibility. You might restrict Web access by categories of sites in the program’s library to prevent them from being exposed to racist, pornographic, or other objectionable materials.

Remember, though, that no software provides perfect protection. Parents need to use a combination of Parental Control software, education, oversight, and communication to protect children, regardless of their age. You can download the TUKI Kid safe browser FREE at www.TUKI.com

Passwords: Get Them & Protect Them
Make sure you have your child’s passwords for email, IM, even social networking sites if you allow them to have access to such sites and programs. It is not recommended for children younger than 13 to have any access to these types of sites and programs. But for your older children whom you may feel are ready to offer such online options, it’s a good idea so you can review who is communicating with your child and in the event of trouble, you’ll
have important access. You can also go the extra mile and put on your best inspector gadget hat! Set up a MySpace, an IM or other account. Learn about it for yourself, explore the safety features available and add your child to your “friend” or “buddy” list. You will not only be able to communicate with your child and be sure they keep their profiles locked on “private” but view comments, posted bulletins, pictures and inappropriate content of others you may want to have your child limit contact with. You never know, you may actually have fun connecting with your child in this new cyber land way!

Also, it is widely known that no one should use easy-to-guess passwords such as names, or dates, social security numbers or other easily obtainable numbers that your child or an Internet hacker might break. There are some computer applications that manage passwords, and some browsers now feature the ability to store multiple passwords. Keep track of passwords in a list on a computer or on paper notes nearby isn’t safe.

**Where Children Use the Internet**

From where do your children currently use the Internet, including e-mail, the World Wide Web or commercial online services?

<table>
<thead>
<tr>
<th>Location</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>70%</td>
</tr>
<tr>
<td>School/Preschool</td>
<td>56%</td>
</tr>
<tr>
<td>Friends/Relative’s Home</td>
<td>9%</td>
</tr>
<tr>
<td>Library</td>
<td>6%</td>
</tr>
</tbody>
</table>

Source: Grunwald Associates

**The Favorites-Sites Kids Love**

Social networking sites like MySpace, Friendster, Facebook, and Xanga are extremely popular with teens. YouTube is popular but a parental concern because there isn’t any filtering for language or adult content. Check with the computer lab administrator at your child’s school to see which ones are used most. Ask your teens if they have accounts (but always try to check for yourself too).

Younger children visit and join hobby sites such as Club TUKI, Webkinz, and Club Penguin. These sites provide games and activities, some (not Club TUKI) include online chat rooms. They are like “cartoon social networking” sites for kids. Club TUKI incorporates an additional element to online safety: education. Club TUKI educates kids via teaching basic reading, finance, math skills and online safety. Whether your kids are teens, tweens, or younger, ask them about which sites are popular with them and their friends. Ask them which ones they’ve joined and have them show you around. You’ll quickly know whether you approve or not.
The Well-Known Risks

Social Networking Sites
Social networking Web sites are among the fastest growing phenomena on the Internet for both kids and adults, but it is tweens and teens who are driving that growth. Among the most popular social networking sites are MySpace, Friendster, Xanga, and Facebook. All of them provide a place for kids to get together online with new and existing friends. When used cautiously, these sites offer great ways for kids to communicate and share their experiences. When used carelessly, however, they can expose your children to identity theft and predators. Teach your children not to post private information or inappropriate or misleading photographs. This information, once posted, becomes public and can be stored on the PCs’ and Internet history files of others. Even if you remove such information or photos, they may still be out there on the Internet and in the hands of people who can use and abuse them.

Social networking sites enable kids to form networks of friends who can communicate freely with one another. Make sure your kids don’t allow people they don’t know to join their networks. They should keep the pages private, so only invited friends can find them on the site. Once strangers are in the network, others in the network will assume a level of trust with them, based upon their relationship with your child. If the stranger is a predator, they may try to take advantage of your child or the friends within the network. Make sure that your child sets the communication features properly so they can approve any postings to their page. This limits even a good friend’s opportunity to post an embarrassing but funny photo, or make a remark you’d prefer Grandma not see!

Porn, Gambling, Racism, Anorexia, and Hate Sites
The darkest corners of the Internet world include some dangerous and illegal elements. Without parental controls or browser filters, it’s almost inevitable your child will run into something you and he/she will find upsetting. Make sure your child knows to tell you when and if that should happen and reassure them you won’t be angry if it does. Some children and teens may become curious about sites featuring racist or hate messages, or promoting risky or damaging behaviors such as anorexia and cutting. You may only discover this by regularly checking your computer’s browser history. Even a single visit should prompt you to talk to your child about it. Don’t assume it was idle curiosity. Explain your house rules about such sites and ask your child about their motivation for visiting. As you talk, if your child reveals issues, such as depression or self-loathing, don’t delay in getting your child professional help from a therapist or other trained specialist to deal with such matters.
Internet Predators
While statistically your child is unlikely to be approached online by a sexual predator, there are enough high-profile cases with tragic outcomes that any parent worries about this. The National Center for Missing and Exploited Children has conducted studies showing that 1 in 7 children will be solicited sexually online, but some of those contacts are from peers, rather than strangers. Make sure your children know they must never email, chat, or text message with strangers and it’s never OK to meet a stranger in the real world. Make sure they understand that someone they see or meet online is still a STRANGER, no matter how often they see them online. A particular worry is for any child that discusses sex with strangers online—this has been shown to lead to even more offline meetings. Should a stranger approach your child online to talk about sex, please visit www.missingkids.com and report it to their Cybertipline. It’s not acceptable to talk about sex with a stranger and any child who has a stranger ask about sexual matters should notify a parent or trusted adult immediately.

Cyber Bullying and Cyber Stalking
Technology gives our children more ways to connect, socialize, and communicate than ever before. Unfortunately, some kids use email, instant messaging, and cell phone photos and text messages to embarrass or bully other children. Also, kids’ digital messages can be edited to change the meaning then forwarded to other kids to embarrass, intimidate, or insult. According to the National Crime Prevention Center (February 2007), 43 percent of children have been a victim of cyber bullying! Make sure your children know they must guard even the most casual text message and watch their own written words. They should never be cyber bullies, and they should always tell you if and when they are being cyber bullied. Keep a copy of any bullying message by using the “Print Screen” key on your keyboard and copying the message into your word processing program. Cyber stalking is a dangerous extension of cyber bullying and used by those who engage in stalking in the real or “offline” world. According to the U.S. Department of Justice, 1 in 12 U.S. women will be a victim of stalking in their lifetime. With awareness of the issue, our older teens can learn to defend
themselves and parents should know how to help. The stalker may hijack an email account and pose as the person whose email they’ve hijacked. The attacker might deface a social networking page or send hateful messages to the victim’s friends, engage in outright identity theft, or try to destroy somebody’s credit and reputation. Cyber stalking is dangerous and should be reported to law enforcement, Internet service providers, and Web site hosts. Keep all evidence of both cyber stalking and cyber bullying.

The Not-So-Well-Known Risks

File Sharing, Music and Video Downloads
Children quickly learn about the joys of sharing music with each other. And it’s often at the tween stage when someone tells them about file-sharing sites, especially the free ones. Let your children know the dangers of file-sharing sites and programs, which let strangers have access to your computer. Using file-sharing sites may expose your computer and information to “bot” software, spyware, keystroke loggers, viruses, and other dangerous malicious code. Additionally, downloading music or videos for free is often illegal. Show your children where they can legally download music and video from sites such as iTunes and Amazon.

Private Information and Identity Theft
Your children don’t automatically know what “private” information is, so you need to explain the concept that it’s any information that allows a stranger access to personal or financial information. Private information includes real world data, name, telephone numbers, address, sports club, school, even the name of a doctor. Bad guys can turn even a small clue into a full record on a child and parent. They, in turn, trade and sell that private data to make money. It’s easy for bad guys to apply for credit in your child’s name and get real world merchandise and money, while ruining the child’s (or your) credit rating and good name. If you do suspect you’ve been a victim of identity theft, you’ll want to monitor your credit report to look for evidence of new accounts or loans. You are entitled to receive one free annual report from each of the three credit reporting services: Equifax, Experian, and TransUnion. It is good to rotate your request from the three firms, every four months, just to make sure your identity and credit are safe. Once you find evidence of identity theft, you will need to report it to law enforcement, beginning with your local police station. That police report will strengthen your case when you work with the other sites and companies involved. You can also put a “freeze” on your credit report and for your children. Visit ftc.gov for more information.
Teen Online Privacy

Educate your teens about the Internet. By now, they are savvy enough (or should be) to know that people online aren’t always who they say they are. It’s easy to lie about your age, sex, and location online so many people do it for innocent and not-so-innocent reasons. Continually remind your teens that they can’t trust strangers online any more than they can in face-to-face contacts. They should never allow a stranger to join a buddy list or a chat or IM conversation. And they should never accept free software, ring tones, or screen savers from strangers. Remind your teen that email addresses, user account names, and IM handles should not be their real name, the name of their school, or some combination of the two; they shouldn’t be provocative or otherwise inviting to a predator. They should be as anonymous as possible. Also, they should never share a password, even with a friend.

Make sure your kid’s school’s Web site is password protected or requires a login for more than superficial, public information. For example, a school in my home town recently posted a travel schedule that included flight information and the names of students traveling for a sports team trip on its Web site. Other possible problems include lists of class names and student addresses and home telephone numbers published on the Web site.

Email and Instant Messaging

Both children and adults should have different email addresses for different purposes. For instance, it’s a good idea to have one address for online shopping, another for online banking, and another for corresponding with friends and family. That way, for example, if you receive a notice from your bank on your family email, you’ll know that it’s malicious spam that you should delete. The same is true for instant messaging. If a child messages or chats with more than
one group, they should maintain different screen names, because predators often follow children from one chat room to another. Make sure your children’s email accounts have the highest level of spam filtering turned on. According to a Symantec research study, 80 percent of children report receiving inappropriate spam on a daily basis. They should use email account names that can’t lead strangers to them.

For example, they shouldn’t use first and last name combinations. They also shouldn’t use suggestive screen names or addresses, such as “playfulgirl” or “wildteen”, even if it seems “cool” to do so. Make sure they use strong passwords that are never shared, even with friends. You should know your children’s email account passwords so you can monitor their activity, frequently. Look at who they send email to and receive email from. Do you know everyone? And let your child know you will be doing this to help keep them safe and not because you don’t trust them.

Key Recommendations:
• Teach children not to click on links within emails that they receive.

• Disable the preview function in email. This prevents potential malicious code in the message area from executing.

• Kids should not respond to emails or instant messages from anyone they don’t know or didn’t expect to receive and block the senders address immediately.

• Never accept a link or download a file through IM.

• They shouldn’t make their instant messaging profile or social networking page public. Always set to private.

• They should always log out when not using IM or when editing their social networking page to make sure their privacy is protected.

Blogging
A blog is an online journal or diary. Some are topical, dedicated to a particular subject matter. Often teens have blogs that are more like traditional private diaries—except they are open to everyone on the Internet via the teen’s own Web site or on a social networking site—which is like placing their diary online for the world to see. Your kids should be sure of their objective in blogging before doing so. Search engines can usually pick up the information that is posted, so your best efforts to protect your privacy are defeated. If you publish photos or links to private Web sites on your blog, you also reduce your privacy.
In addition, people such as potential employers or school admissions officers may read your blog, and this exposure may affect other areas of your life as well. For example, people interviewing for jobs have been declined because of items in their personal blogs or in the blogs of friends and family that mention them. Don’t let your teen become a blog victim.

**The Newest Threats**

**Got Bot?**
“Bots” and “botnets” are now becoming some of the latest threats to emerge from the dark side of technology. Bots (short for robots) are forms of stealth software that can sneak into your computer and cause it to send out spam and phishing emails to others. Bots have become so common, it’s estimated by Symantec’s Security Response Center that 11 percent of U.S. computers are already infected! Many illegal businesses now thrive on these bots that can spread like wildfire among hundreds of thousands of unsuspecting personal computers for the sole purpose of stealing your personal information and cheating you out of your hard earned money.

**How Do They Do It?**
A bot is a type of malicious software, snuck onto your machine by cyber-criminals, allowing the attackers to take control over your affected computer. These “Web robots” are usually part of a network of infected machines that are used to carry out a variety of automated tasks, including the spreading of viruses, spyware, spam, and other malicious code. Worse, the bots are used to steal your personal information and wreak havoc on your credit including the unauthorized use of your credit cards and bank accounts. The bots can also display phony Web sites, pretending to be legitimate, and fooling you into transferring funds and providing your user names and passwords to be used for more illegal activity.

The best defense against these horrible little bots is to install top-rated security software (Norton™ AntiBot is a good choice) and be sure to set your software’s settings to update automatically so you know you’re getting the latest protection. The experts also advise that you never click on attachments or links inside emails unless you can verify the source, which is something you need to teach your kids.

**Signs of Internet Addiction**
MMORPG—what is that? It stands for the increasingly popular and potentially addictive “massive multiplayer online role-playing games.” Titles such as World of Warcraft, Lord of the Rings, and
Everquest are currently popular. These can be highly immersive and for some teens, especially boys, a real distraction from their real lives. Set rules with your children about the amount of time that can be spent on these sites, whether or not they get money to spend for membership or to purchase gaming accessories (in the real world, such as on eBay or within the game) and any other concerns you might have.

According to the Computer Addiction Services at Harvard University-affiliated McLean Hospital, these are some of the psychological and physical symptoms of addiction:

- Inability to stop the activity.
- Neglect of family and friends.
- Lying to employers and family about activities.
- Problems with school or job.
- Carpal tunnel syndrome.
- Dry eyes.
- Failure to attend to personal hygiene.
- Sleep disturbances or changes in sleep patterns.
Have your kids learn internet safety playing games at www.ClubTUKI.com
What’s Best For Your Children at Any Age

Elementary School Children (ages 5-7)
This is the age when many of today’s children are introduced to the Internet. Now that more and more U.S. schools have computer labs, PCs or Macs in the classroom, a child’s first use of a computer may be at school. Others often get their first computer experience at home, learning from parents or older siblings. According to the U.S. Senate resolution naming June as Internet Safety Month, 35 million U.S. children from kindergarten through grade 12 have Internet access, and 80 percent are online at least 1 hour per week. Young children are often completely engaged by simple games and educational sites, but they will quickly learn about new sites from their peers. Web sites—such as Neopets, Webkinz, and Club Penguin—start by ages or 8. We refer to these as entry-level social networking sites because many have chat and other communication features. Parents of young children should turn these features off initially.

It’s difficult for children of this age to understand the “stranger danger” associated with someone contacting them through the friendly interface of a favorite game or club site. Later you can introduce the concept of chatting with people they know, such as aunts, uncles or friends—being sure to reinforce that they should always ask you before talking to anyone online. Ideally, when your children are this age, you will be actively involved with their online activities the same way you are with their homework. For example, you should make sure the computer your child uses is within your view.

---

### Internet Spurs Learning Activities

<table>
<thead>
<tr>
<th>Currently, what are the main uses of the Internet in your home?</th>
<th>How often do you use the Internet for schoolwork</th>
<th>How often do you use the Internet for general learning activities not connected with school?</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERCENT SAYING EDUCATION/LEARNING FOR CHILDREN</td>
<td>CHILDREN AGES 9 TO 17</td>
<td>CHILDREN AGES 9 TO 17</td>
</tr>
<tr>
<td>Parents</td>
<td>Children Ages 9 to 17</td>
<td></td>
</tr>
<tr>
<td>53%</td>
<td>48%</td>
<td>52%</td>
</tr>
<tr>
<td>At Least Once a Week</td>
<td>At least Once a Month</td>
<td>28%</td>
</tr>
<tr>
<td>Parents</td>
<td>Children Ages 9 to 17</td>
<td>33%</td>
</tr>
<tr>
<td>28%</td>
<td>At Least Once a Week</td>
<td>24%</td>
</tr>
</tbody>
</table>

Source: Grunwald Associates
Parental control software can help you by limiting the sites your child can access, even when you aren’t around. The controls also limit any information you don’t want your child sharing, whether it be their name, age, phone number or any other private information. You should turn on all the filtering and security features in your computer’s search engine (such as Google’s “SafeSearch” feature, found under “Preferences”) to prevent your young child from inadvertently arriving at an adult or other inappropriate site as they do their homework. Be sure to show your child how to close a browser window and let them know it’s always OK to close a site if something surprising or disturbing occurs. Tell them never to chat, type messages or share information with anyone on these sites unless you are with them.

**Key Recommendations:**

- Limit approved Web sites and hours spent online.
- Set high security settings with browsers, membership, and social networking sites.
- Install and maintain Internet security software and parental controls.
- Use parental controls to limit the Web sites your child can visit.
- Monitor your child’s computer use and sit with them when they’re online.
- Talk about protecting private information (name, phone number, etc.) and never sharing passwords with friends.

**Tween Children (ages 8-12)**

Tween children are far more social and adventuresome in their computer use. They talk to their peers at school and learn about the newest and “coolest” sites. They might sign-up for their first email and instant messaging accounts. Ask your child about those accounts and what the passwords are, so that you can monitor their activities, and know with whom they are communicating. Children at this age may also start to check out social networking sites, such as MySpace, Facebook, and Friendster that are popular with older teens and adults. Most won’t create a page until they are a little older, but they will visit, join, and chat with friends, older siblings, and other relatives who have their own pages and profiles.

Tweens are also interested in music, and the Internet is an easy way to listen, discover and download new tunes, as well as meet others who share their musical interests. They might follow news about a favorite group or celebrity by visiting their blog or Web
site and checking out different sites to get the latest gossip along with downloadable photos. Online video sites, such as YouTube! Are enormously popular. Many of the videos contain strong language or violent material, so you need to monitor your tween’s visits carefully. The more creative tweens are learning how to take their own digital photos, edit videos, and share their creations with friends and family. With your help or the help of a more experienced friend, they are starting to post their creations online as well.

Key Recommendations:

• Frequently check your computer’s Internet history to see the sites your children have visited, and monitor their email and instant messaging accounts to see who they communicate with.

• Set rules about online communication, illegal downloading, and cyber bullying.

• They should know to never click a link in an email or IM—this is a common way people get viruses or reveal private and valuable information to criminals.

• Discuss risks and concerns about posting and sharing private information, videos, and photographs.

• Watch for signs of obsessive or addictive online behaviors (see Online Gaming and Signs of Addiction).

• Keep computers in a common area in the house.

• Foster open communication and encourage your kids to tell you if anything online makes them feel uncomfortable.

Teens (ages 13-17)
Teens are developing ever greater independence and this is reflected in their online lives. With that independence comes responsibilities, including being careful in their online world. Yes, at these ages, teens have usually formed or joined online worlds such as MySpace, Friendster, Facebook and others. With screen names, memberships, blogs, profiles, and other Internet elements that they visit daily, teens communicate the details of their lives with each other. Digital traces of their thoughts can be left all over the Web. Often they don’t know—or they forget—that everything posted on the Web is there for all to see, and it’s probably there indefinitely. All it takes is a single Google search by a college admissions director or potential employer—five, ten, even twenty years from now—and all of the photos, opinions, and thoughts of your teen are there or all to see forever. Caution is so important!
Key Recommendations:
• Reinforce rules of appropriate online behaviors (language, private information and imagery, cyber ethics, illegal downloading, limiting hours of usage, and avoiding inappropriate adult sites).

• Be aware of your teen's online life (social networking sites, photographs, private information, club and sports activities) whether on their site, a friend's site or their school's Web pages.

• Review the sites your teen visits; don’t be afraid to discuss and possibly restrict sites that offend or concern you.

• Remember your teen is accessing the Internet at home, school, a friend’s house, the library, via cell phone, or even a gaming system—so talk to your teen about their activities in all those scenarios.

• Ask them not to download files (music, games, screensavers, ringtones) or make financial transactions without your permission.

• Teach them to never share passwords and be wary about typing private information when on a shared or public computer, or one they think might not be secure.

• Teach them to never click a link in an email or IM—this is a common way people get viruses or reveal private and valuable information to criminals.

• Keep computers in a common area in the house and not in your teen's bedroom.

• Foster open communication and encourage your teen to tell you when something online makes them feel uncomfortable. Remember, they are teens but they are still kids.

College Bound Teens
As your teen grows up and leaves home, whether for school or work, they will need to understand the additional adult responsibilities to be found in the online world. That includes protecting their privacy, especially their social security number and financial information; preventing identity theft; and related risks to their credit history, which is particularly important for a young adult. If your teen is using a laptop at college or in their new job, make sure they understand the added risks of using wireless connections and that they purchase the necessary security software including a reliable backup solution. They might be tempted to skip these optional items, so it’s good to insist on vigilance when it comes to their laptop's security.
Have your kids learn internet safety playing games at www.ClubTUKI.com
3 Simple Rules to Follow
(courtesy of iKeepSafe.org)

Parents:
• **Keep Current** with technology. You don’t have to be an expert, but a little understanding goes a long way towards keeping your family safer online. Get basic technical training and learn about new products as they get released. Visit www.norton.com/familyresource to stay up-to-date.

• **Keep Communicating** with your children about everything they experience on the Internet. Learn their lingo, and ask them when you don’t understand something. Work to keep your communication lines open.

• **Keep Checking** your children’s Internet activity. Know where they go online. Let them know that you’ll keep checking because you love them, and you want them to understand that the Internet is a public forum and never truly private.

Kids:
• **Keep Safe**: Keep your personal information safe—all of it! Never give your real name, address, phone number, the name of your school, or a picture of yourself to anyone online.

• **Keep Away**: Internet strangers are dangerous—STAY AWAY. No matter what anyone tells you, NEVER meet anyone in person. You have no way of knowing who they really are. Don’t talk with them online, and never tell them where you live.

• **Keep Telling**: Tell your parents or a trusted adult about everything you see on the Internet. Always tell them when something makes you feel uncomfortable. Remember, not everything you see and hear on the Internet is “true” or even “normal.”

Remember…
Until now, this dilemma has been complicated by a shortage of credible information. There was a lack of good data about where children access the Internet, what they do once they’re connected, what kinds of sites they visit, and how much adult supervision and guidance they receive, among many other basic issues. Nor did we know much about parents’ perceptions of and expectations for their children’s Internet usage. Without sound research, there is a tendency to react to the headlines and hype of the moment – and that tack may not result in wise school policymaking and parental oversight.
Today credible data has been collected via a significantly large random sample of households nationwide to learn about children’s Internet usage and gained valuable insight for a much needed, overdue reality check on the role of the Internet the lives of our youth.
Have your kids learn internet safety playing games at www.ClubTUKI.com