

## **Pornography**

Children or teens may accidentally access online pornography. It is necessary to seek to prevent this through effective computer security, discussed above, and education. It is essential that your child or teen know exactly what to do to limit what they see if such accidental access does occur. Never punish your child for accidentally accessing this kind of material.

Protect your younger child by making sure that all sites accessed are ones that you have reviewed or are accessed through a school or children's library web site. Closely supervise any open explorations. Tweens and teens must know how to surf safely. Simple guidelines for tweens and teens are:

- Don't click on a link, if you do not know what it will access.
- Don't type a URL. Type the name of the site in a search engine.
- Don't open suspicious email messages or click on links in email messages unless you are absolutely sure they are legitimate.

All children must know that if "yucky" material appears online, they should immediately turn off the monitor and get your help. Tweens and teens may should turn off the monitor, force-quit the browser, or turn off the computer. The computer security and incident should be reviewed to prevent future incidents. Praise your child for his or her effective response.

## **Cyberbullying**

Prevent your child from being victimized by cyberbullying by ensuring that your child does not post information that could be used against him or her and by paying attention to the quality of your child's online community.

Make sure your child knows to never retaliate if cyberbullied and to save the harmful material. Your child may be able to handle some situations alone by calmly telling the cyberbully to stop, ignoring the cyberbully, or filing a complaint with the web site. Make sure your child knows he or she should ask for your help if these steps do not work or the cyberbullying is significant. Other response options include sending the online material to the parent of the cyberbully with a demand that it stop, working with the school to address the situation, and contacting an attorney or the police.

Deter your child from engaging in cyberbullying by emphasizing the importance of treating others kindly online and through effective monitoring. If you receive a report that your child has been unkind online, take proactive steps to ensure this does not continue.

## **Focus on the Positive**

Most young people are having fun and having healthy interactions with others online. As long as their online activities remain balanced with other important life activities, the sites they are regularly using have good standards, and the people they are engaging with are safe, these activities can benefit their lives and deepen their understanding of themselves, their friends, and the global community. Internet risks and concerns can be effectively managed through education and careful parental attention.

Quite simply, we cannot prevent young people from engaging in cyberspace. We must prepare them to do so safely and responsibly.

# **Cyber-Safe Kids Cyber-Savvy Teens**

## **Helping Young People Learn to Make Safe and Responsible Choices Online**

By Nancy Willard

Author of: *Cyber-Safe Kids, Cyber-Savvy Teens:  
Helping Young People Learn to Make Safe and  
Responsible Choices Online*

## Introduction

The Internet provides wonderful opportunities and is clearly an important vehicle for information-sharing and communication. The Internet is enhancing our society. But there are dark sides to this wonderful resource that can present risks and concerns for the well-being of young people.

The reality is that there are risks online and some teens are making unsafe or irresponsible choices that are resulting in harm to themselves or others. But young people also face risks in the Real World? Sharp knives, speeding cars, bullies at school, weirdos at the park, drug pushers, and more. And sometimes they simply do not make good choices.

Keeping children and teens safe online requires applying effective Real World parenting skills to cyberspace. When children are young, we keep them in safe places and teach them simple safety rules. But as they grow, we provide them with the knowledge, skills, and values to independently make good choices — and remain “hands-on” to ensure they do.

These same strategies should be applied to the online world. When children are young, they simply do not have the cognitive development or experience to keep themselves safe online. Parents must establish a safe online environment and provide children with simple, easy to follow guidelines.

But as children grow and their online activities expand, it is necessary to make sure that they know how to independently make good choices. Teens need to know what the risks are. They must know how to avoid getting involved in a risky online situation, how to detect if they are at risk, and how to effectively respond. And they need to care — they need to understand that it is important to keep themselves from harm, make sure their friends are safe, and not cause any harm to someone else. Lastly, because they are teens they are still likely to make mistakes or engage in inappropriate activity. Or someone dangerous could be manipulating them. So parents must pay attention to what teens are doing online.

Recently, there has been a significant amount of fear-mongering about the Internet. As a result, many teens have become more reluctant to talk with adults about online activities — especially if they have become involved in a difficult situation. They fear that adults will overreact, blame them, and restrict their online access. We must do a better job of developing a trusting relationship between adults and young people related to Internet use.

This brief guide will provide an overview of Internet risks and concerns, recommended parenting approaches, and information about strategies to address foundational issues and key online safety concerns.

© 2007 Nancy Willard. This booklet may be copied and distributed for non-profit purposes. More resources are available on the *Cyber-Safe Kids, Cyber-Savvy Teens* web site at <http://cskcst.com> and on the Center for Safe and Responsible Internet Use site at <http://csriu.org>.

## Don't Take Candy From Strangers

### Ensuring Stranger Literacy

Children and tweens should be protected against communications with online strangers, except in very well moderated environments.

Teens can be expected to engage in interactions with people who they do not know or know only as an acquaintance. The vast majority of online strangers or acquaintances are perfectly safe — but some are not. Unsafe online strangers include sexual predators, people who are “recruiting” for dangerous groups, and other people who want to engage teens in unsafe or unwise activities. All teens must learn to determine the safety and trustworthiness of an online stranger or acquaintance. Some teens will want to meet with someone they have met first online and must know how to do so safely.

Teens must know the RED FLAGS! **“Watch out for anyone, especially an adult, who sends overly-friendly messages, tells you how special or wonderful you are, offers gifts or opportunities, tries to establish a special or secret relationship, asks for a sexy picture, or tries to turn you against your parents or friends. These are signs of danger!”**

### Addressing Specific Safety Risks

Address the following specific safety risks with your child:

#### Sexual Predators

Predators almost always target teens, and not children. Teens can more easily be groomed to meet to engage in sex and can more easily travel for such a meeting. All teens are not equally at risk from sexual predators. Predators are looking for teens who post information online that reveals they are emotionally vulnerable or they are exploring sexual issues or their sexual orientation. They also specifically seek teens who post sexually provocative images, use sexually inviting usernames, or go to chat rooms or sites where people discuss sex and arrange for sexual “hook-ups.”

- Pay attention to all material that your child is posting to make sure none of indicates any level of vulnerability or sexual interest. Make sure you know your child’s social networking friends and IM buddies.
- Your child must know to watch out for the online stranger danger Red Flags and respond appropriately. If your child does tell you about an inappropriate contact, it is absolutely critical that you do not overreact. Acknowledge and applaud their detection and response to potential danger.
- If you suspect that your child is communicating with a predator, it is safest to contact the police and not inform your child that you are doing so.

#### Scams

Young people should be taught to be very wary of any opportunities that are: “Too good to be true” or advise: “Act now or you will lose out.” These are key indicators of a scam. They must know not to provide personal contact or financial identity information online without your approval. They also should know that virtually ALL offers for free “goodies,” contests, and chances to win a prize online are techniques to obtain personal contact and interest information that will be retained and used for advertising to them.

## Keeping Life in Balance

### Preventing Internet Addictive Behavior

Internet addictive behavior is an excessive amount of time spent using the Internet, resulting in lack of healthy engagement in other areas of life — school, work, time with friends and family, and sleep. Young people who get sucked into a life spent primarily online are highly vulnerable to many different risks. Social networking sites can be very addicting for those teens who are highly concerned about their social status and relationships with peers. Online gaming sites, especially multiplayer, role-playing games, are also highly addictive.

Children and teens absolutely need to be spending time with their family and with other young people — engaged in sports activities, the arts, social service, or just “hanging out.” Parent involvement is necessary to ensure that these Real World interactions occur. Do not allow the Internet to be your child’s “baby-sitter.” Time spent online should only be a small part of your child’s life.

If your child is spending too much time online, develop a mutual agreement about the amount of time to be spent online and strategies to support engagement in other activities. Use time limiting software to support this arrangement, if necessary.

Young people also often engage in media-multitasking while doing homework. Make sure your child is not surfing, gabbing, or gaming online when there is homework to be done. This can significantly interfere with effective learning.

### Read With Your Eyes Open

#### Enhancing Information Literacy

There are no “Cyberspace Truth Monitors.” It is necessary for young people to learn how to determine the credibility of material provided on Web sites or in messages. Too many people determine credibility based on appearance — which can be very deceptive. Steps to effectively assess credibility include:

- Consider how important it is that the information be credible.
- Assess how controversial the issue is, because this could affect bias.
- Reflect on how you got to a site or received the information.
- Evaluate the source of the information looking for potential bias and what the source is seeking or has to gain if you agree with their information or position.
- Determine whether the information is fact-based or opinion-based.
- Determine whether the information is consistent with information found through other sources.
- Ask for the opinions of others.
- Evaluate the information itself.

## What are the Risks and Concerns?

Internet risks and concerns range from situations where innocent young people are victimized by others to situations where young people have engaged in actions that are risky, irresponsible, harmful, and even illegal.

### Safety Risks

#### Sexually Related Risks

- Being groomed by predators for sexual activities or to provide pornography.
- Accidentally accessing online pornography.
- Receiving sexual harassment.

#### Cyberbullying or Online Social Aggression

- Being the target of harmful material that is sent or posted online.

#### Scams and Identity Theft

- Being deceived by an online scam, including financial identity theft.

### Responsible Use Concerns

#### Risky Sexual Activities

- Intentionally accessing pornography in an addictive manner.
- Seeking sexual “hook-ups” with adults or other teens.
- Engaging in sexual harassment.
- Posting or sending sexually provocative or explicit images.
- Discussing and sharing images of sexual exploits publicly.

#### Cyberbullying or Online Social Aggression

- Harming another by sending or posting harmful material online.

#### Unsafe Communities

- Interacting with online communities that support self-harm, including cutting, anorexia, and suicide.

#### Dangerous Groups

- Interacting with angry and violent online groups, including hate groups, gangs, or troublesome youth groups.

#### Cyberthreats

- Posting material that raises concerns about violence or self-harm.

#### Online Gaming

- Excessive involvement in online games, especially violent games.

#### Online Gambling

- Engaging in “gambling 101” game activities or actual online gambling.

#### Hacking

- Breaking into or damaging computer systems.

#### Plagiarism

- Inadvertently or intentionally using online information resources in an academically dishonest manner.

#### Copyright

- Inappropriately copying or disseminating someone’s copyrighted work.

## Specific Online Activities

Some risks are associated with specific online activities or technologies.

### Commercial Online Activities

Commercial Web sites are actively involved in market profiling and advertising. They encourage young people to disclose vast amounts of personal information that is used to tailor advertisements based on their known interests. Young people may be offered “gifts or prizes” in exchange for completing online marketing surveys.

Advertisements may promote unhealthy consumption, lifestyle, values, and behavior. Some promote junk food and passive entertainment products, which can lead to obesity. Some are overtly sexual. Advertisers may encourage young people to think that having certain products is necessary to be considered “cool” and encourage them to nag their parents.

There are three online advertising techniques that parents must recognize and teach their children to recognize:

- **Advergaming:** Advertising is integrated into online games and activities. Young people likely do not recognize these games as advertisements.
- **Permission marketing:** Asking young people to sign up to receive advertising information in the form of newsletters and coupons.
- **Viral marketing:** Encouraging young people to promote products and services to their friends.

Web sites use specific strategies to enhance their “stickiness” to entice young people to spend lots of time on their site, generally so they can see more advertisements. This can foster addictive access behavior.

### Social Networking Sites

Social networking sites allow teens to express their personal identity and maintain electronic connections with friends. Teens create profiles and blogs to share their interests and thoughts, establish friendship links, and engage in public or private discussions. There are many positive aspects of social networking. The most popular social networking sites have excellent terms of use agreements, practices to allow users to have control over who has access to their information, and a procedure to file complaints.

Unfortunately, some teens are disclosing inappropriate material on these sites, including personal contact information, sexually provocative material, intimate personal information or materials that can damage their reputation and future opportunities. Some make unsafe connections with dangerous individuals or groups. Some engage in or are targeted by cyberbullying, including sexual harassment. Some become highly addicted to the online interactions. Many appear to consider the number of friendship links as a measurement of self-worth. Tweens may lie about their age to participate.

### Chat Rooms and Discussion Groups

Chat rooms and discussion groups allow teens to discuss issues within a group of acquaintances or strangers. The level of safety depends on the location or site, the subject, and whether there is a moderator.

## Protection Strategies

There are four key strategies for children and teens that provide the essential foundation for safe and responsible Internet use: privacy, addictive behavior, information credibility, and stranger literacy.

### None of Your Business

#### Addressing Privacy Concerns

Some teens are revealing significant amounts of personal information online. They appear to be unaware of the public and possibly permanent nature of their online disclosures and how such disclosures may place them at risk, damage their reputation, or interfere with their future education and career plans. Some appear not to understand that information shared privately through electronic messages can easily become very public. Teach your child that different kinds of personal information must be handled differently:

#### Personal Contact and Financial Identity Information

Personal contact and financial identity information should only be provided on a secure site for an appropriate purpose. Make sure your child knows not to post such information without your permission. Teach your older teen how to provide such information safely on secure sites. This information includes: full name, address, phone number, and any personal identification or financial account number. Your child should also be careful about disclosing a personal email address, although many times this is necessary.

#### Intimate Personal Information

Intimate personal information is private information that should generally remain confidential. Intimate information should never be shared in public locations, such as social networking sites. Publicly posting this kind of information can place your child at high risk. Although there is some risk, it may be appropriate to share intimate information in a private message with a very trustworthy friend or on a professional online social support service.

#### Reputation-Damaging Material

It seems illogical that there is a need to remind teens that it is not smart to post or send material could damage their reputation or that others could use against them — but this is necessary cautionary guidance.

#### Personal Interest Information

Personal interest information is more general information about personal interests and activities. In most online locations, it is generally safe for teens to share this kind of information. This is the kind of information teens can post in profiles, on Web pages or in blogs, and the like. But they should know that commercial sites use this kind of information to target advertisements. They should avoid providing personal interest information in response to a survey, as this will be stored in a database and be used to direct advertising to them.

#### Personal Information About Others

Your child should know that the personal information about other people is their business and should not be shared online, publicly or privately.

## Detecting and Responding to Concerns

The key “red flags” that something might be going wrong online include:

- Appearing emotionally upset during or after Internet use.
- Disturbed relationships with parents, family, or friends.
- Spending too much time online, especially late at night.
- Excessively secretive behavior when you approach the computer or an empty history file. (Teens are likely to be somewhat secretive.)
- Receipt of packages or phone calls under strange circumstances.
- Subtle comments about online concerns. It is very important to respond carefully to such comments. Remain calm and try to encourage your child to talk further. Your child will likely be worried that you will overreact.

If you discover online concerns:

- Do not overreact! Take the time to calm down before doing anything, especially discussing your concerns with your child.
- Investigate further. Use monitoring software if you think your child is at risk.
- Carefully try to engage your child in a conversation about Internet activities.
- Seek professional assistance, if warranted.
- Respond to unsafe or irresponsible behavior with an appropriate consequence that will remedy any harm and help your child learn make better choices in the future.
- If you find evidence of a predator or other dangerous individual, do not confront your child. Contact law enforcement.

## Making Good Choices Online

Support your child in making good choices online by emphasizing important values and standards. Ask your child to review the standards set forth in the school Internet use policy and the terms of use agreements for sites and services and note how these standards are similar to your family’s values.

Use “teachable moments,” like news articles or specific incidents, to discuss online issues and problem-solving strategies. Teach your child to ask questions to guide responsible decision-making. Questions like:

- “Is this kind and respectful to others?”
- “How would I feel if someone did or said the same thing to me, or to my best friend?”
- “What would my mom, dad, or other trusted adult think or do?”
- “Would I violate any agreements, rules, or laws?”
- “How would I feel if my actions were reported on the front page of a newspaper?”
- “What would happen if everybody did this?”
- “Would it be okay if I did this in Real Life?”
- “How would this reflect on me?”

Encourage your child to talk with his or her friends about their online choices. Emphasize to your child the importance of reporting to you, or another trusted adult, if he or she witnesses online harm or thinks that someone is making or considering a bad choice.

## Instant Messaging

Instant messaging (IM) is real time electronic communications. The level of safety depends on who is included on a young person’s contact list.

## Cellphones and Personal Digital Devices

Today’s young people are becoming totally wired — able to access the Internet anytime, anywhere. This limits adult’s ability to effectively supervise.

## Digital Cameras, Cellphone Cameras, and Web Cams

Young people can easily capture and send images. These images can also be electronically modified. Inappropriate images posted online by your child or others could damage your child’s reputation, attract the attention of an unsafe person, or be used in the context of cyberbullying.

## General Internet Safety Guidelines

General guidelines to support safe and responsible Internet use include:

- Discuss values and standards regarding online activities frequently.
- Effectively address computer security.
- Keep the computer in a public area of your house, so you can peek over your child’s shoulder frequently.
- Establish standards regarding Internet use when you are not present.
- Encourage high-quality online activities.

## Protection Technologies

### Computer Security

Parents must ensure that all family computers have adequate computer security, including firewalls virus and spam protection, and blocks against pop-up ads. Do not allow peer-to-peer networking on any family computer. Set your search engine preference to filter search results.

### Filtering Software or Parental Controls

Filtering software may provide some protection against accidental access. Limiting access to approved bookmarked sites for younger children and teaching teens how to avoid accidental access are better strategies. Filtering software will provide no protection or deterrence whatsoever for a determined teen. Focus on imparting values and periodically checking the history files.

### Time Limiting Software

Time limiting software can help to limit access when you are not present.

### Monitoring Software

Monitoring software could interfere with the establishment of a relationship based on mutual trust. However, it might be very useful if your child is not willing to discuss online activities or has engaged in online wrong-doing — or if you fear your child is in danger from someone online.

## Internet Use Through the Ages

### Younger Children

Younger children should only use the Internet in safe places — Web sites that you, teachers, or librarians have found to be appropriate. Make it easy for your child to access his or her special bookmarked sites. Any electronic communications that are allowed should be limited to known friends. Three simple guidelines for children:

- Don't go outside the safe online places without an adult.
- Never type your name, address, or phone number on the computer.
- If something "yucky" appears, turn off the screen (make sure your child know how) and tell an adult.

### Older Children

Start involving your older child in deciding what sites are appropriate and why. Introduce safety and responsible use issues in a manner consistent with your child's development and online activities. Restrict communications to known friends or well-moderated sites.

### Tweens

Recognize that tweens and early teens are most vulnerable online. Many tweens want to participate in online social networking, which is not advisable. But most tweens know they can lie about their age to register on sites for users over the age of 13. Allow your tween more freedom in finding new appropriate sites, emphasizing safe searching techniques. Increase discussions of risks and concerns. Continue restricting communications to known friends or on well-moderated sites.

### Early Teens

Consistent monitoring and discussions about Internet issues are imperative during this time period. Prior to allowing participation in "over age 13" sites, make sure our child has a good understanding of protection strategies. If your child registers on a social networking site, review the profile settings to make sure your child's profile is private, there are limits on who can communicate with your child, and any postings of material by others on your child's profile are pre-approved by your child before being made public. Regularly review all individuals your child has included as a friend or an IM buddy. Allow more freedom and engage in less monitoring as your child demonstrates good choices. Work with the parents of your child's friends to develop common Internet use standards.

### Older Teens

By the time your child is 16, he or she should be know how to independently use the Internet in a safe and responsible manner. This gives you two years of "fine-tuning" before your child leaves home. Allow your child to earn the right to have Internet access in his or her room by demonstrating the ability to make good choices online. But make sure your child gets to bed on time and continue to periodically check the history file.

## Monitoring Online Activity

Parents should pay close attention to what children are doing online. Teens naturally are more concerned about personal privacy. Teens will argue that their posts on social networking sites are part of their private lives. Public posts are not private. Here is how you can explain your monitoring:

"It is necessary for me to make sure you are making good choices online because I am your parent and I am responsible for you. I will periodically review your history file and your postings in public places. Remember, what you post in public is public. As I see that you are making good choices, I will be able to reduce this monitoring. I will review your personal communications only if I have reason to suspect something is wrong. In most cases, I will discuss my concerns with you before any review."

### Making Bad Choices Online

It is important to consider why teens might make bad choices online. These are some of the reasons:

#### "Didn't think."

- Teen's brains are a "work in progress." They are developing the capacity to engage in effective decision-making. This requires paying attention to the consequences of your actions, which is difficult to do online.

#### "You can't see me."

- Teens perceive they are invisible online, or they can take steps to be anonymous. This reduces concerns of detection, which might lead to disapproval or punishment.

#### "I can't see you."

- Teens do not receive tangible feedback about the consequences of online activities. This interferes with empathy and a recognition that their actions have caused harm.

#### "Who am I and where do I fit it?"

- The major life task for teens is establishing their personal identity, values, and relationships with others. This can lead to inappropriate activities.

#### "If I can do it online, it must be okay."

- Teens may forget that Real Life values should control their online choices.

#### "Everybody does it."

- Other teens and adults are making bad choices online.

#### "Looking for love."

- Teens who face temporary or continuing challenges — including personal mental health issues, difficulties in school, and/or challenges in relationships with family or friends — are at high risk online. They are not likely to pay attention to obvious risks or make good choices. They are highly vulnerable to manipulation by dangerous individuals or groups.

#### "Doing what they say."

- Dangerous individuals and groups, as well as commercial sites, use sophisticated techniques to immanipulate online users.

## **To those who have downloaded this document.**

Yes, you may reproduce and distribute this document, as long as you do so without charging anyone for it. It must also be reproduced in full, not portions.

If you work with teens, you might also want to review the companion Teen's Guide.

This booklet has been designed to be reproduced back-to-back on 3 pages of 8 1/2 X 11 paper and folded - thus forming a 8 1/2 by 5 1/2 booklet. It will be necessary to turn pages 2, 4, and 6 a different direction to get this to reproduce correctly.

The pages should appear in the following order:

Cover

Introduction

None of Your Business

Read With Your Eyes Open

Don't Take Candy From Strangers

CyberbullyNOT

Don't Hook Up With Online Losers

Avoid the Porn

Too Good to Be True

Watch Out for THEM

What You Do Reflects on You

Additional resources will be added to the *Cyber-Safe Kids, Cyber-Savvy Teens* web site. Additional information resources and opportunities for professional development are available on the Center for Safe and Responsible Internet Use site at <http://csriu.org>.