

# What You Do Reflects on You

Making Good Choices Online

## ***You Can't See Me - I Can't See You***

Some teens make bad choices online. They think they are invisible and won't be caught. They might not recognize the harm to others or themselves. Others may manipulate them. Some teens are "looking for friends in the wrong places" and end up finding the wrong kinds of friends.

## ***Values and Standards***

Try an experiment: Write down a list of the values and standards you have learned from your parents about making safe and responsible choices. Get a copy of your school's Internet use agreement. Download the Terms of Use agreement from your favorite social networking site. Compare them. You will likely find that the values and standards are very similar. Ask yourself why.

## ***Good Choices Questions***

Here are some questions you can ask yourself to make good choices online:

- 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?

## ***Friends Don't Let Friends Make Bad Choices Online***

Talk with your friends about online risks and responsible online behavior. If you know someone is making an unsafe choice or is in danger online the person will not listen to you, tell a trusted adult.

# Cyber-Savvy Teens

## Making 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

No one has to tell teens how fun the Internet is or how important it is for you to use the Internet to connect with your friends. You are also probably aware that many adults have concerns about teen safety online – as well as growing concerns about whether teens are behaving responsibly. You have likely seen the news reports:

*Teen exposure to online porn!*

*Cyberbullies causing emotional harm!*

*Young people solicited by online sexual predators!*

*We need to block MySpace and YouTube!*

You might have shaken your head and said to a friend, “What gives? I’m not doing anything wrong and I feel safe online.”

The Reality: There are some risks online and some teens are making unsafe or irresponsible choices online that are resulting in harm to themselves or others. But there are also risks in Real Life – like sharp knives, speeding cars, bullies, weirdos at the park, drug pushers, and more. Sometimes teens don’t make good choices in the Real World.

So how do you handle risks and make good choices online? First, you need to know what the risks are. Then you need to know how to avoid getting involved in a risky situation, how to detect if you are in at risk, and how to effectively respond. Lastly, you need to care – you need to understand that it is important to keep yourself from harm, make sure your friends are safe, and not cause any harm to someone else.

That is what this booklet is about.

- The basics: Protecting your personal privacy, keeping your life in balance, assessing the credibility of online information, and determining the trustworthiness of online strangers.
- Key safety concerns: Predators, cyberbullies, pornography, and scams.
- Other important issues: Making good choices on social networking sites, understanding commercial aspects, copyright and plagiarism.
- Personal responsibility: Watching out for online “manipulators” and making good choices online.

© 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://cscst.com> and on the Center for Safe and Responsible Internet Use site at <http://csriu.org>.

# Watch Out For THEM

## Manipulators Online

Dangerous individuals and groups, as well as commercial sites, may use sophisticated manipulation techniques to influence your attitudes and behavior.

### **Manipulation Techniques**

“Manipulators” frequently use the following techniques. Watch out for any person, organization, or web site that ...

- Offers or gives you a “gift.”
  - A gift can be an item, praise, or offer of an opportunity. When an Manipulator gives or offers you a gift, it makes you feel like you must give something in return.
- Asks for your commitment.
  - “Be my friend.” “Be part of our team.” Manipulators will ask for your commitment, then make you feel you must remain true to that commitment.
- Encourages you to go along with a group.
  - People tend to follow what a group decides to do. Manipulators will specifically encourage people to go along with others.
- Tries to create a really attractive image.
  - Manipulators can use the Internet to create a positive, attractive image. They want people to like them - and then do what they ask.
- Creates a misperception of authority or expertise.
  - Manipulators want people to think they are “the boss” or the “expert” - so people will do what they say. They use the Internet to create this image.
- Threatens a loss if you do not act fast.
  - “Act now, or you will lose out.” By threatening a loss, Manipulators encourage people to act fast without thinking.

### **Trust Your Gut - Take a Closer Look**

If you think someone is trying to manipulate you online, you may be right. What you will likely feel is a “gut reaction” that something is wrong. Trust your gut reactions and be sure to take a closer look. Is someone trying to manipulate you?

Make a commitment to do what is right and what is best for you, not what THEY say.

# Respect the Source

## Plagiarism

Plagiarism is presenting material created by someone else as your own work. At its essential core, plagiarism is simply a lack of respect. Students may plagiarize intentionally or inadvertently. In either case, this can lead to a failing grade or other sanctions.

### ***Intentional Plagiarism***

Students may intentionally plagiarize when they have not gotten their homework done on time. Your primary “job” as a student is to get your school work done.

- Make sure your other activities do not get in the way of doing your school work well and on time.
- Don’t leave important work on major writing projects to the last minute.

### ***Inadvertent Plagiarism***

Some students may inadvertently plagiarize the work of others because they don’t know how to keep track of their references or cite properly. Here are some strategies that can help:

- When you start a writing assignment, create a “resource” folder and a “citations” document. Save all the original documents you are going to use in the folder. Paste the reference on your “citations” document, including the URL.
- Create a “notes” document. You can “cut and paste” material from your resource documents into this “notes” document – but make sure you keep track of the citation. Organize your notes into an outline for your paper.
- Rewrite the material in your own words. Or you can occasionally use specific quotes – but make sure you quote properly.
- Go over your final draft and make sure you have included all of the appropriate citations for the material you have rewritten or quoted. If you have lost a citation, you can easily find it in your “citations” document.

### ***Wiki World***

It is important to cite your sources whenever you post information online. Many people are now jointly creating materials in wiki environments. Make sure you include proper citations when you post material in a wiki.

# None of Your Business

## Online Privacy Protection

Always remember that any information you send or post online is public – or could easily be made public. Different kinds of personal information must be handled differently.

### ***Personal Contact and Financial Identity Information***

Full name, address, phone number, cell phone number, any personal identification numbers, or passwords.

- Post only on a secure site for an appropriate purpose with parent approval.

### ***Intimate Personal Information***

Private, sensitive personal information – personal diary information.

- Never share publicly. Probably safe to share on a professional online support service site – but check the site carefully. May be safe to share in a private message with a **very** trustworthy friend – but be really careful.

### ***Reputation-Damaging Material***

Information or images that could damage your reputation and future opportunities (college, job, relationship) or that others could use against you.

- Do not post or send online – publicly or privately.

### ***Personal Interest Information***

General information about personal interests and activities.

- Generally safe to share, but ask your parents.

### ***Personal Information About Others***

Personal contact, intimate, or reputation damaging information about your family, friends, or other people.

- Do not post or send online. You have no right to share their information

### ***Protect Yourself on Social Networking Sites***

Many social networking sites now have features that allow you greater control over your personal information. But all of your friends can still view the information you post in public places on your profile.

- Follow the above guidelines, even if you are using the privacy features. Because if your friends have access, it is not really private.

# Keep Your Life in Balance

## Internet Addictive Behavior

Online activities can be fun — but don't let time spent online take the place of all of the other activities that also can make your life healthy and enjoyable.

### ***Addictive Access Questions***

The following questions can help you determine whether the time you spend online is interfering with other important activities:

- Do you frequently find that you have spent more time online than you were planning?
- Do you use the Internet late into the night?
- Are you frequently tired at school because you were online late into the night? Are you using lots of caffeine drinks to get through school?
- Do you spend time online instead of doing homework, reading, hobbies, chores, physical activities, or spending time with friends or family?
- If you are not online, are you thinking about the last time you were online or making plans for the next time you will be online?
- Do you argue about time limits your parents have set for Internet use? Or do you use sneaky ways to get around these limits?

### ***Keep Your Life in Balance***

If you answered “yes” to many of the above questions, then you are showing signs of Internet addictive behavior. You will be happier if you can bring your life into balance.

- Make a commitment to spend more time with your friends and doing fun activities that do not involve “screens.”
- Set goals for the amount of time you will spend online and keep track of your time. Use a timer if you think necessary.
- Avoid surfing, gabbing, or gaming online when doing homework. This can really interfere with your ability to learn the material and do a good job.
- Make sure you get to bed on time.

# Respect The Creator

## Copyright

Copyright laws protect important values: The rights of people who have dedicated time and creative effort to create something new to control how others use their creative work. The benefit to society of having new creative works.

### ***Copyright Basics***

- Under copyright law, the creator of a new creative work – writing, music, art, photograph, and the like – has the right to control the ability of others to reproduce, distribute, revise, perform, or display that work.
- Most copyright owners protect their creative work with a copyright notice: © 200\* Name of creator.
- Some creators make their works available through a “creative commons” approach. They give permission for certain kinds of uses, such as use for non-profit purposes. See: <<http://creativecommons.org>>.

### ***Respecting the Rights of Creators***

- If you want to reproduce, distribute, revise, perform, or display a work created by someone else, you can only do so if:
  - The work is in the “public domain” – a very old work, created by a government agency, or placed in public domain by the creator.
  - You have permission to use the work – either directly from the creator or a notice granting permission that appears on the work.
  - Your use is considered “fair use” – you are using only a small amount for educational or criticism purposes and your use will not cause financial harm to the creator.
- Make sure you do not infringe on the copyright rights of others when you post material online.
- Purchase copyrighted entertainment media – music, games, videos, and software – from legitimate sources.

### ***Copyrights Are Your Rights***

The Internet allows everyone to create and publish their own works. Use a copyright notice to protect your creative efforts. You can also provide a notice on your work if you are willing to allow others to use the work in limited ways.

# Eyeballs and E-Wallets

## Market Profiling and Advertising

Commercial Web sites think teens are “hot prospects.” They know you spend lots of money and convince your parents to spend even more money. They want to get through your eyeballs and into your e-wallet.

### ***Getting to Know All About You***

Web sites want to know all about you – your age, gender, location, interests, and purchasing habits – so they can use this information to advertise to you. This is called “market profiling.” They keep this information in a database.

- How do they obtain your information? They retain information you provide during registration, track your online activities, review what you have posted, and encourage you to complete market research surveys. “Are you hip?” questionnaires and online contests are also market research surveys.
- There is no way to prevent companies from obtaining some of this information. But make your own choice about giving them even more information by completing questionnaires or other market research surveys.

### ***Are You “Cool?”***

Advertisers want you to think that to be “cool” you must have their product or use their service. Another message they frequently promote is that only “sexy” girls and “macho” guys are cool.

Make sure you recognize these online advertising techniques:

- Advergaming: Integrate ads into online games and activities.
- Permission marketing: Ask you to sign up to receive newsletters or become a “friend” on a social network profile that is really just an ad.
- Viral marketing: Encourage you to promote products or services to friends.

### ***Sticky Business***

Commercial sites try to be really “sticky” – to entice you to spend lots of time on their site, so you can see more ads. This can lead to addictive access.

### ***Make Your Own Choices***

Ads are the price we pay for free Web sites. Just don’t let the advertisers shape your values and behavior in ways that are not healthy. Be your own self. Make your own choices.

# Read With Your Eyes Open

## Information Credibility

There are no “Cyberspace Truth Monitors.” Anyone can post any information online, whether it is true or not. Be careful to determine the accuracy of any material you see online. Don’t judge the accuracy based on appearance of the site.

### ***Information Credibility Questions***

The following are questions you can ask to determine whether online information is credible and accurate:

- How important is it that the information be true and accurate? The greater the importance, the more care you should take.
- How controversial is the issue? The more controversy about the issue, the greater the possibility of bias or different opinions.
- How did you get to the site or receive the information? Information you found following a link from another highly credible site is likely credible. Information on sites found using a search engine may vary in credibility. Information in an unsolicited email message is likely not credible.
- How credible is the source? Carefully evaluate the site to determine if the source of the information is legitimate.
- What does the person or group that posted the information have to gain if you agree with their information or position? Is someone trying to sell you something or gain some other objective? Information on sites that are trying to sell something or gain support for a cause could be more biased.
- Is the information fact-based or opinion-based? Opinion-based information could be more biased.
- Have you found the same or similar information on other sites or in books or magazines? The more places, both online and offline, you can find the same or similar information, the higher the probability of accuracy.
- Who else links to the site? Paste the URL directly into a search engine and you can find who links to the site. Then you can assess the credibility of the people who think that the information is accurate.
- What do others, especially a parent, teacher, or librarian, think? If you have any questions be sure to ask others.
- Is the information consistent with what you know to be true? This is the “gut reaction” test.



# Don't Take Candy From Strangers

## Stranger Literacy

The vast majority of online strangers 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. It is exceptionally important to be very careful in determining the safety and trustworthiness of anyone you first meet online and to be very, very careful if you want to meet with an online stranger in person.

### ***Determine the Safety of Online Strangers***

- Carefully review the person's online presence. Look closely at the material posted, who the person's friends are, and how the person communicates.
- Consider how you met this person and the basis of your relationship.
- Take time to get to know people online. It is hard to keep a facade.
- Pay attention to details of messages and watch for inconsistencies.
- Ask others for their opinion. What does a trusted friend think?
- Save and report any communications that raise concerns.

### ***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! Show any messages like this to an adult.**

### ***Safely Meeting in Person With an Online Stranger***

- NEVER agree to meet without a safety plan and your parent's approval.
- Any meeting should be in a public place, with your parent or trusted friends nearby. (Make sure your trusted friends have told their parents.)
- Make sure you have a cell phone. Pre-arrange a safety check phone call from your parent about 5 minutes into your meeting.
- Never leave the public place with the stranger.

# Me and MyFriends

## Social Networking Safety

Social networking sites are places to express your personal identity and maintain electronic connections with friends. There are many positive aspects of social networking.

### ***Check It Out***

Before you join a social networking site, check it out:

- Do you meet the age requirement to participate on this site?
- Do the terms of use prohibit harmful activities?
- Does the site allow you to control who has access to your page?
- Does the site have a complaint process?

### ***Protect Your Privacy and Reputation (and Friends)***

- Use the privacy protection features to limit who can view your profile.
- Even if you use privacy protection features, don't post material that could ...
  - ▷ Allow a stranger to find you in Real Life.
  - ▷ Attract a dangerous stranger.
  - ▷ Be used by a cyberbully to torment you.
  - ▷ Damage your reputation, friendships, or future opportunities.
  - ▷ Cause harm or distress to another.
- If you see that a friend has posted any of this kind of material, talk with your friend about the risks.

### ***Be Selective***

- Be selective about who you add as friends Remember the old saying: “You are known by the company you keep.” Would you feel comfortable introducing this person to a close friend or your parent? It is perfectly okay to turn down a request for a friendship link or remove a friendship link because the person does not fit in with your values.
- Don't make the mistake of thinking that having a large number of friendship proves you are an important or popular person.
- Communicating with friends online can strengthen your friendships. But make sure you also spend time with your friends in Real Life.

# Too Good to Be True

## Online Scams

Online scammers try to get your personal contact information, financial information, or entice you to participate in questionable, possibly illegal, activities.

### **Scam Indicators**

Watch for anyone who tells you ...

- “Free lunch!” You can get something really great for very little work or risk.
- “Act fast!” You must act now or you will lose your chance.

These are important indicators that someone may be trying to scam you.

### **Kinds of Scams**

Specific scams to watch out for:

- Contests to win a prize or a notice you have won a prize. This is a very common strategy to obtain personal contact information. There is NO prize!
- Ways to earn money that require little or no work.
- Offers to help you get a college scholarship.
- Email messages that threaten that if you do not verify your financial account, you will not be able to access your account.

### **What Do Scammers Want**

Scammers generally want to get your personal contact information and financial information. They could try to involve you in illegal activities.

### **Protect Yourself**

- Learn when it is safe to provide personal contact information and how to safely engage in electronic commerce. Always ask your parent.
- Never provide personal contact information or financial identity information, if there are any indicators of a scam.

### **Market Profiling Scams**

ALL offers for free “goodies,” contests, and chances to win a prize online are techniques to obtain personal contact and interest information. This information will be retained in an individualized market profile database and used to send you advertising. It could be used for other scam activities.

# Don't Hook-Up With Online Losers

## Online Sexual Predators

Online sexual predators are older people, generally men, who are using the Internet to form relationships with teens that will ultimately result in sexual activity. Online sexual predators may also try to get teens to send them sexually explicit images.

### **Predator Techniques**

Online predators look for teens who are vulnerable or who show signs they are interested in or have questions about sex. They use techniques called “grooming” to manipulate and seduce teens. They are very friendly, offer many compliments, and may offer gifts or opportunities. They will try to become a teen’s best online secret “friend” and interfere with a teen’s relationships with others. When they have established trust, they will start to talk about sexual issues. They want teens to think of them as a “sexual mentor.” Some teens are embarrassed to report these interactions, because the predator has manipulated them into talking about or engaging in sexual activities. You must understand that predators are master manipulators.

### **Don't Attract Online Losers**

Don't do things online that could attract a predator. Don't post sexually provocative images, join online groups to discuss sex, share intimate personal information or information that makes you appear to be vulnerable.

### **What You Must Know**

- Sexual predators are not lovers or mentors. They are abusers and losers.
- Meeting with a sexual predator could result in sexually transmitted disease, forced engagement in risky sex, abduction, and even murder.
- Help get rid of these online losers. Save all evidence of any contact by a possible predator and report to a trusted adult, the Web site or service, the police, and the agency in your country that handles these reports.

### **Friends Don't Let Friends Hook-up With Online Losers!**

If you think a friend has become involved with an online sexual predator, encourage your friend to report, even if your friend is embarrassed to do so. If your friend is not willing to report, tell a trusted adult. Your friend is at risk!

# CyberbullyNOT

## Online Social Aggression

Cyberbullies use the Internet or cell phones to send hurtful messages or post information to damage people's reputation and friendships. They are "mean kids" online.

### ***Don't Put Yourself at Risk***

- Don't post or send information others could use against you.
- Pay attention to how you are communicating. Be careful not to insult others.
- Don't hang around online places where people treat you badly.

### ***If You Are Cyberbullied***

- DON'T RETALIATE! This only gives the cyberbully a "win" and could make other people think you are part of the problem.
- Save the evidence and try to figure out who the cyberbully is.
- Decide whether you can handle the situation by yourself or should tell an adult. But if what you try does not work, be sure to get help from an adult.
- Depending on how bad the cyberbullying is, the steps you or a parent can take include (you will need your parent's help for some of these steps):
  - Calmly and strongly tell the cyberbully to stop and to remove any harmful material or you will take further action.
  - Ignore or block the communications.
  - Send the material the cyberbully has posted to his or her parents and tell them to make it stop.
  - File a complaint with the Web site, ISP, or cell phone company.
  - Get help from your school counselor, principal, or resource officer.
  - Contact an attorney to send a letter or file a lawsuit against the parents.
  - Contact the police if the cyberbullying includes any threats or is a crime.

### ***Friends Don't Let Friends Get Hurt Online***

Take action if you see that someone is being cyberbullied. Tell the cyberbully to stop, help the person being cyberbullied, or tell a trusted adult.

### ***Don't Be a Cyberbully***

It's not "cool" – it's cruel.

# Avoid the Porn

## Accidental Access of Online Pornography

Teens sometimes accidentally access online pornography. It is important to understand and avoid the "traps" pornographers create to get people to access their sites.

### ***Basic Safety Rules to Avoid Porn***

- Read, think, then click.
  - Never click on a link unless there are good indicators that the link will go to an appropriate site. If in doubt, don't click.
- Don't type URLs.
  - Some porn sites use URLs that are similar to popular sites hoping that people will mistype the URL. Type the name of the site you want to access in a search engine and then carefully evaluate the search return to make sure you are accessing the right site. (This is also a good strategy to avoid identity theft.)
- Watch out for porn spam.
  - Don't open suspicious email messages. Never click a link in an email message unless all indicators are that the link is safe.
- Keep your computer safe.
  - Don't download peer-to-peer networking software. P2P is a source of spyware and other malware (malicious software) that can deliver porn.
  - Configure your browser to block pop-up ads and your search engine to "safe search."
  - Make sure your parents have installed effective computer security tools.
- Turn it off and report.
  - If inappropriate material appears on the screen, turn off the monitor, force quit the browser by holding the Control-Alt-Delete keys, highlighting the browser name, and clicking "End task" or "Force quit," or simply shut down the computer.
  - Always promptly report accidental access – so that concerned adults will know this was a mistake and you will not get into trouble.
  - After any accidental access, someone with computer expertise should evaluate the computer and how the accident happened to make sure corrective actions are taken, like removing cookies or malware.



**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 parents, you might also want to review the companion Parent'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

Me and MyFriends

Eyeballs and E-Wallets

Respect the Creator

Respect the Source

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>.