

Safe and Responsible Online Behaviors for Children

Shu-Hsien L. Chen

Assistant Professor
Graduate School of Library & Information Studies
Queens College, City University of New York
Flushing, New York, U.S.A.
E-Mail: slchen@qc.edu

Abstract

The Internet makes new learning opportunities possible for children by offering vast amount of resources and powerful communication means. Oftentimes, the Internet is the first resource children choose for information seeking. Other than schoolwork related resources, the Internet contains unlimited interesting and entertaining information for children. As going online becomes a favorite pastime for millions of children, teachers and parents need to caution children about the negative side of the Internet. They need to teach children online safety and responsibility, and further, monitor their online behaviors. The article, first, discusses the possible threats to children's online safety, including potential sex offenders, pornographic materials, and unethical marketing tactics aimed at children. Then, it addresses unethical and irresponsible behaviors, such as plagiarism, spamming, and hacking, which are committed or may be committed by children. Finally, the article explains how teachers and parents can help children become responsible and ethical Internet users.

Keywords : *Internet; Computer ethics; Online safety; Spamming; Plagiarism; Hacking*

Introduction

The advent of the Internet in K-12 schools during the 1990s has opened up new possibilities for innovative teaching and learning in an electronic environment. Integration of the Internet into curriculum has changed traditional practices of instruction in classroom. The World Wide Web provides teachers and students with a wealth of resources located worldwide, and enables them to search information anytime and anywhere without being restricted by time and space. Additionally, e-mail, bulletin board, and chat room, the powerful communication means, expand students' physical territory and shorten their distance with the world by connecting them rapidly with peers across the town, experts in the nation, or pen pals around the world. Via the instantaneous Internet connectivity students go into an unknown world, where they see, listen, learn, and explore many fun and new things, as they have never experienced before. To many school children, the Internet represents not only a huge source of useful and valuable resources,

but also an interesting information mall where they can chat or hang out with their online buddy, and enjoy an array of rich and sensory multimedia experiences.

Lately, the Internet has become a fairly common technology tool employed in numerous schools and homes. It has been reported that 99% of public schools in the United States had access to the Internet during the fall of 2001, and among these schools 87% of classrooms had Internet connection.¹ The ratio of students to instructional computers connected with Internet was 5.4 in 2001 as compared to 12.1 in 1998. Many schools, especially, large schools and schools with the lowest poverty concentration gave students Internet access outside regular school hours. Thus, children are provided with an adequate technology environment to access the Internet. In addition to school Internet, many children and teens also have Internet connection at home. The 2000 census showed that two thirds of homes with a child between the age of six and seventeen owned computers, and 53% of homes subscribed to Internet services.² A more recent report of the U.S. Department of Commerce indicates that more than 60% of families with children have Internet access at home.³ As Internet connectivity has been steadily increasing in recent years, a majority of children and teens have access to the Internet at school and/or home.

Indeed, the Internet offers many benefits for teachers and students. No other technologies can surpass the Internet in the amount of resources it offers, besides, with its speed of information delivery, timely information, and level of interactive nature, the Internet is highly valuable and appealing resource to teachers and students. Teachers and students communicate and network with people easily through e-mail; they can also access enormous amount of information simply by a few clicks. In spite of the benefits of the Internet, it has a negative side that teachers and parents should alert their children. They need to teach students safety measures while navigating the Internet, and further instruct them to develop responsible and ethical online behaviors. Students must know how to safeguard themselves from harmful individuals or potential pitfall, and at the same time they must be responsible and ethical Internet users. In light of importance of the topic, this article will discuss online safety and responsibility for children. Unethical and irresponsible behaviors: plagiarism, spamming, and hacking will also be addressed. Finally, it will delineate that teachers and parents both play a vital role in helping children access the Internet in a safe and responsible manner.

1 National Center for Educational Statistics, "Internet access in U.S. public schools and classrooms : 1994-2001," [Online] Available : <http://nces.ed.gov/pubs2002/intemet> (Accessed April 3, 2002).

2 A. Poftak, Net-wise teens : Safety, ethics, and innovation," *Technology & Learning*, 23 : (2002) : 36-49.

3 W. Minkel, "Media literacy-part of the curriculum," *School Library Journal*, 48 : (2002) : 31.

Safety

Even though the Internet has already become a very popular tool in countless schools and homes, many children have not fully developed concepts of proper online behaviors. Often teachers and parents voice their concerns about children's online safety, yet the safety issues have not been deeply rooted in their minds. Children lack critical thinking and problem-solving skills to differentiate what are acceptable or not acceptable behaviors on the Internet partially because they are still in developmental stage mentally and emotionally. The pervasiveness of the Internet, unfortunately, does not accompany their understanding of safety issues. In the invisible cyberspace children feel a false sense of safety while communicating in the chat room, corresponding with e-mail, or navigating Web sites. They tend to believe what they read, see, or hear; consequently, they become easy targets for online advertisement or suspicious individuals lurking around the cyberspace. Based a survey on online safety conducted among 565 children between the ages of 6-18, 34% of them considered it was all right to meet someone they had been chatting online; and 28% thought nothing was wrong to reveal their real names in a chat room.⁴ While 23% of these children had no qualms giving their address, another 23% would do the same with their pictures.

As noted, the number one Internet feature for children is its powerful communication means. Fifty-six percent of children created more than one e-mail address so that they might assume different roles to communicate in different ways.⁵ As children expose themselves more frequently on the Internet without taking precautions, they become more vulnerable to online predators or pedophilias. Sixty percent of students admitted that they had been contacted by online strangers.⁶

Children are subject to several types of risk as they go online. The most common type is inappropriate Web sites filled with indecent materials and lewd graphics. Children's access to pornography and their communication with strangers are the constant concern of parents. Teachers are equally concerned about students' proper use of the Internet at school. Child pornography sites mushroom rapidly. It has been reported that there are at least 100,000 child pornography sites,⁷ and the number may be steadily growing. In addition to child pornography sites, pornographic materials are dissemi-

4 L. Joseph, & S. Ward, "Youth views of online safety," *USA Today*, (August 15, 2002), p. A1.

5 *Op. Cit.*, Poflak.

6 *Op. Cit.*, Poflak.

7 J. Nordlinger, "Spam tastes gross," *National Review*, 54 : (2002) : 36-39.

nated over the Internet via e-mail by spammers. Often after children participate in the chat room or message board, their mailboxes are suddenly flooded with countless annoying junk e-mail. Children and teens may intentionally access inappropriate sites out of curiosity; they may unintentionally stumble into the sites or fall into the victims of spamming. Regardless of the different circumstance, they must be taught how to handle such embarrassing and unpleasant incident.

Pornography is by no means a new problem existing only in this technological society; it has been with us in the traditional print world. Nevertheless, the easy accessibility of pornography on the Internet by children and viewing them in the privacy of their bedrooms certainly complicate the control issue of children's access. As long as the Internet is an uncharted and unsupervised territory, anyone can post text, images, graphics, audio, video, and animation on the Internet without going through the strenuous process of being screened and reviewed as required by print publishers. Consequently, children's awareness of potential online dangers and their self-governed behaviors is one of the most effective ways to safeguard their own safe and responsible behaviors on the Internet.

Another type of potential danger comes from sinister individuals who prey on naive children playing on the Internet. Lurking around the Internet under the security of anonymity, some deceptive adults may pose themselves as a child and teenager to communicate with other youngsters in the chat room or by e-mail. After these individuals have earned the trust and friendship of children, they then request children to meet them. They may even send bus fare or airline tickets, sometimes cameras for children to take pictures of themselves. We all have heard about familiar stories of a man disguising himself as a teenager to chat with children on the Internet, then trap them, and exploit them sexually. A detective named Jim McLaughlin hunt down 280 sex offenders in 43 states and 15 countries by impersonating himself as a vulnerable teenager on the Internet, and he got all of the offenders convicted.⁸ Julie Posey is another advocate for child safety on the Internet. She takes it upon herself to look for suspicious individual in the cyberspace.⁹ She monitors the Internet looking for predators and pedophiles, and receives tips from people about suspicious activity that they have found. She follows up the information, identifies the suspects, and passes the information to law enforcement for further investigation. Her work has caused 20 arrests and convictions.

Another type of risk pertains to Internet marketers who use questionable practices toward children in order to sell products or to collect personal

8 T. Fields-Meyer, & A. Driscoll, "Not the girl he seems," *People*, 58 : (2002) : 79-80.

9 *Op. Cit.*, Nordlinger.

information. Advertising in child-based Web sites has been rapidly growing in recent years as consumer businesses see great spending power of children and teens. In 1995 alone, children under 12 spent \$14 billion, teenagers another \$67 billion.¹⁰ Online marketers employ several tactics to target children and teens. Children may be lured into filling out forms or registration that asks personal information when participating in a contest sponsored by Internet marketers.¹¹ Some Web sites entice children with free items if they provide personal information about their families. Collection of children's personal information can also occur when they play online games. A recent study of the U.S. Federal Trade Commission reported that 89% of 212 children's sites collected personal information directly from children, less than 10% of the sites offered some sort of parental control over such information collection.¹² Kids' clubs are also one technique employed by online advertisers to generate brand loyalty for their products. Oftentimes children join the clubs by typing in personal, even family information online without seeking parental approval beforehand, thus how to interrupt children's online actions at the right moment becomes difficult for parents. Parents have not been consulted about their children's online decision; as a result, they cannot take adequate measures in time to protect their children's privacy or family's personal information. The Web sites of some companies offer children nothing educational or entertaining in value but advertisement only. Worst of all practices, online marketers utilize one to one marketing technique with children in order to establish personal relationships with them and hold their attention for a long period of time.

Many children do not have critical thinking skills, clear analytical abilities, and adult mental maturity to make proper judgment as they are surrounded with irresistible commercial temptation. They may not realize the information given by them to an advertiser or the game played by them is actually a data collection technique of advertisers for business purpose. Also, many children are not able to distinguish clearly between entertainment and marketing because the content and advertising become seamlessly integrated.¹³ Moreover, they may have difficulties to distinguish the difference in advertising and the interactive game of the Web site.¹⁴ Because of vulnerability of children, advertisers should take into consideration their age and maturity. Some Web sites do consider children's age and maturity when

10 J. Azoulay, "Is online on the line? Kid-based websites," *Children's Business*, 13 : (1998) : 23-27.

11 M. J. Austin, & M. L. Reed, "Targeting Children Online: Internet advertising ethics issues," *Journal of Consumer Marketing*, 16 : (1999) : 590-602.

12 Jim Teicher, "An action plan for smart internet use," *Educational Leadership*, 56 : (1999) : 70-74.

13 Center for Media Education. (2003). [Online] Available : <http://www.cme.org> (Accessed March 15, 2003)

14 Federal Trade Commission. [Online] Available: <http://www.ftc.gov> (Accessed March 15, 2003)

asking personal information. For example, Barbie site advises children to seek parents' approval to use the Web site and also to type in the child's user name and a parental password. They allow children to see a variety of products and play interactive games. Unfortunately, many Websites do not exercise ethical practice ethical toward children and teens.

Because of vulnerability of children, Center for Media Education, Direct Marketing Association, and The Council of Better Business Bureaus have jointly set up some guidelines for practicing ethical and responsible marketing.¹⁵ The guidelines state children should be honestly told so when they are being targeted for a sale. Parents' permission is required for placing orders, and they should be allowed to cancel unwanted orders placed by their children. If personal data are being collected, reasons for collection should be explained at the level of language that children can understand. Parents' permission should be obtained before collecting personal information. Also, advertisers should also provide a way for children to discontinue receiving e-mails if they desire to do so.

Unethical and Irresponsible Behaviors

Indeed, the Internet offers children unlimited learning opportunities and abundant resources, and often it is their favorite source for information seeking. It is a free territory, where children often spend long hours navigating Web sites with little or no supervision of parents or teachers. Thus, to be safe and responsible on the Internet has become critical issue. Children need to stay away from pornographic materials, and watch out for suspicious strangers and clever online marketing practices. They must observe proper online guidelines and be ethical and responsible information users. On one hand, to benefit from vast amount of resources and rapid communication means, children must be aware of potential dangers hidden on the Internet before they go online. On the other hand, children may unintentionally turn themselves irresponsible and unethical Internet users because of ease of copying information from the Internet. It is very easy for students to submit a class assignment, which basically consists of a copy work from Websites. Using other's ideas or writing as one's own without giving proper credit is common practice of many students. The anonymous nature of the Internet could also boost up their false sense of security, tempting them into acting harmfully toward others. Under the disguise of invisibility in the cyberspace children could change their personalities and carry out things that they dare not do in this physical world. The irresponsible and unethical behaviors for children come in many forms; the discussion of the article will be limited to

15 *Op. Cit.*, Austin, & Reed.

plagiarism, spamming, and hacking. Other unacceptable behaviors such as shouting and flaming, and others are listed in Top Ten Netiquette Tips in Appendix B.

Plagiarism

“Plagiarize” is defined as “steal and pass off the ideas or words of another as one’s own” and “use another’s production without crediting the source.”¹⁶ To plagiarize is to commit literary theft. It is by no means a new problem in this technology world; it has been with us since we use written language to record human experiences. Nevertheless, plagiarism has never been so easier in today’s digital environment. With a few clicks on a computer, students can cut and paste, complete and turn in a research paper in no time at all. To many students, writing a paper is no longer an active mental process, which requires them to gather, use, evaluate, synthesize, organize information, then communicate in writing, and finally submit the paper. Critical thinking and analytical skills play no role while they take other’s ideas and writing as their own. The serious consequence of plagiarism could be a failing grade or expulsion from school, but the most serious consequence is the infringement of intellectual property of original authors.

Plagiarism or cheating among students is increasing. In a survey of educators, when asked whether the Internet makes plagiarism a greater problem, 48% of 951 educators indicated plagiarism increased while 13% said that it dramatically increased.¹⁷ Only 5% of them did not consider plagiarism a problem. When the Internet provides students with plethora of information, many take advantage of it and choose a shortcut to complete their assignments. Based on a survey conducted by the Center for Academic Integrity at Duke University, 70% of 4,500 students admitted seriously cheating on written work, and 52% stated they cut and pasted verbatim from Web sites.¹⁸ Do they know it is wrong to do so? “Yes, it’s wrong. But it’s easier, so I don’t care.” said a high school freshman.¹⁹ Students might wait until the last minute to do a research report, and in the wee hours under pressure of meeting deadline, they download an entire paper from the Internet to pass it as their own work. Plagiarism by no means exists only among teenagers. It affects younger students as well. It is not so unusual to see children submit a computer printout as their assignments.

Students may not realize plagiarism is a form of theft, i.e. stealing other’s intellectual property. Also, they have no clear concepts of what constitutes plagiarism. Ignorance of serious consequence resulted from plagia-

16 “Plagiarize,” *Merriam-Webster Dictionary*, [Online] Available: <http://www.m-w.com> (Accessed April 1, 2003).

17 E. Colkin, T. George, & T. Kontzer, “Teens ace it shortcuts,” *Information Week*, 879(2002) : 55.

18 *Op. Cit.*, Colkin, George, & Kontzer.

19 *Op. Cit.*, Colkin, George, & Kontzer.

rism could contribute to their careless attitude toward plagiarism. Therefore, preventive education must be given to discourage students from copying other's words, taking other's ideas as one's own work, or downloading software, music from the Internet. Students need clear guidelines on using film clip, music, and software in their multimedia projects. Before assigning a research paper or project, teachers need to give students instruction on proper way of using printed work or non-print resources. Students must be told in unequivocal language that the following behaviors are considered plagiarism:²⁰

1. Using other's work and submitting it as one's own.
2. Copying other's words or ideas without giving credit or acknowledgement.
3. Quoting other's words or writing without using a quotation marks.
4. Giving inaccurate information about the source of a quotation.
5. Copying sentences except making a few changes of words without giving credit.
6. Majority of the work consisting of other's words or ideas from a single source.

Oddly enough, while teachers deplore the increase of plagiarism, there exist Web sites or paper mills, which offer students a term paper for only \$5 to \$10 or even without charge.²¹ Cheating in schoolwork is made not only easy but also cheap for students. On the other hand, the Web site <www.turnitin.com> claims that it can help teachers identify cheaters and prevent digital plagiarism. The Web site <turnitin.com> is used by numerous high schools and universities around the world, and recently, it was chosen to provide plagiarism protection for every post-secondary institution in England. Another Web site <plagiarism.org> is designed to provide on-line resources for educators, and give facts about Internet plagiarism and a report on the growth of "cheatsites" online.

Spamming

With rapid communication capability and low cost of information transmission, people use e-mail to replace postal mail. However, the advantages of e-mail communication such as easiness, convenience, and instantaneousness in sending out message have been utilized to promote business, advertise products, and even to disseminate indecent materials over the Internet. The most common messages, services, or products advertised by spammers include chain letters, get-rich-quick schemes, easy loan and low interest

20 "What is Plagiarism," (2003). Turnitin. Corn [Online] Available: <http://www.turnitin.com> (Accessed March 13, 2003).

21 *Op. Cit.*, Colkin, George, & Kontzer.

mortgage, quick weight loss, online prescription, quack health products and remedies, and initial stock offerings for unknown start-up corporations.

Simply put, spamming is a large volume of junk e-mail or unsolicited commercial e-mail sent indiscriminately to Internet subscribers by individuals or business to promote products or services. In most circumstances, spammers have no contact or interaction in real life with their e-mail recipients. Spammers collect e-mail addresses for bulk mailings by gathering them from Web pages, usenet newsgroup postings, online directories, and responses to online advertisements. AOL subscribers are especially vulnerable to junk mail because harvesting e-mail addresses from AOL takes no much effort. As AOL users participate in chat rooms or on message boards, their users' names appear there. So junk mailers can easily collect addresses, compile into databases, and sell to other junk-mailers. The would-be spammers also purchase software to acquire e-mail addresses.

Spamming is hard to combat for spammers are clever and persistent. They use tricky tactics to bombard people's inboxes in spite of their efforts to refuse them. To prevent the junk mail from being deleted, spammers use misleading subject lines, such as "Sorry I missed your call." or "Do I have the correct address." Upon seeing such subject lines, potential receivers tend to think that the e-mail comes from an acquaintance or an old friend. To avoid being traced the origin of the junk mail or being filtered and blocked, spammers often route their mail or advertisement through a third party's server without permission. Sometimes they hijack someone's e-mail address to issue junk mail, and cause a flood of angry responses to the poor victim. Either utilizing a third party's server or other's mail address, spammers or junk mailers send bulk of junk mail without cost while transferring financial burden on ISPs for expand the broadband and storage capacity to hold junk mail. Worst of all, spamming tarnishes the reputation of companies, and at the same time cause endless annoyance to their victims.

Children could be the victims of spamming after they open their own e-mail account and make first visit to the chat room. Many schools do not allow students to have school e-mail account to prevent junk mail and other management problems. Before opening an account, children need to be cautioned about the possibility of receiving junk mail and pornographic materials via e-mail. Guidelines on how to deal with junk mail should be given beforehand. Teachers and parents must instruct children that they never send money, give out credit card or personal information to any business or individuals unless they have consulted with their parents or teachers and gained their prior approval. They must understand that offers of money-making opportunities, beauty improvement, or magic cures described in e-

mail are simply too good to be true. Oftentimes spammers use false e-mail address to issue unsolicited commercial mail. So the message is bound back when recipients return the mail or request to be removed from their list. If there is really a valid e-mail address, recipients can forward copies of junk mail to spammers' ISPs, and indicate their desire not to be bothered with unsolicited mail. Most ISPs want to maintain their reputation so they take copies of forwarded junk mail messages seriously.

There is a potential risk of contracting vicious virus to cause destruction of data or the hard drive when opening junk e-mail with attachments. Because of deceiving subject lines, recipients may be tricked to open seemingly innocent e-mail. Merely e-mail message cannot carry a virus, but an e-mail attachment that contains a computer program can carry a virus.²² Therefore, opening junk e-mail will not do much harm except wasting one's time, but opening e-mail attachment containing a computer program can result in serious damage or destruction. Children can protect themselves from virus contamination by deleting mail coming from unfamiliar and suspicious senders who advertise products and services. Though the problem of spamming is hardly found among children, they certainly can be the victims of spam messages. They could also receive a chain letter, continue its cycle, or they may initiate a chain letter to annoy many recipients. Children must be warned that sending a chain letter as well as shouting and flaming are considered unacceptable behavior in netiquette (See Appendix B).

Hacking

A hacker means someone who breaks into a computer system to read e-mail and other files. In the world of hackers, there is distinction between different types of hackers.²³ Hackers considered avid computer enthusiasts are those who gain illegal entrance to a system for intellectual stimulation or mental thrill but with no ill intention. Instead, they may do so to have something to brag about. Crackers, another type, enjoy breaking into a system and seeing the system go haywire. The most dangerous hackers are those who break law simply for money. They break into the computer systems of banks or financial institutions, and transfer money to different accounts. We read reports of hacking by teenagers or adults in news or media, but seldom find news about getting into financial institution because it may adversely encourage copycats.

Many teen hackers are merely curious and bored. The invisibility coupled with anonymity in the cyberspace gives them a false sense of security to get into an unauthorized computer system, snoop around, and poking

22 A. Clyde, "E-mail is wonderful, but...", *Teacher Librarian*, 26 (1998) : 56-58.

23 K. Komando, "Hackers and crackers," *Popular Mechanics*, 176 (1999) : 62-67.

around. Though they have no intention to alter data and files of a computer system, their action could cause interruption of normal functions in an organization or institute. They may not realize seemingly innocent and mischievous behaviors could become harmful and constitutes a crime. In the cyberspace, where teens are in total control for the first time, their personality could suddenly change and become obnoxious, aggressive, and irresponsible. Several years ago, America Online network was hacked by teens, who reportedly used homemade software tools to create free AOL accounts, fake credit card numbers, and even obtain access to AOL personnel files.²⁴ Jon Johansen, a teenager in Norway, was arrested because he and two co-writers created a program to decrypt DVDs so that he could view DVDs on computers.²⁵ Back a few years ago, a Boston-area teen crashed a phone company's network; as a result, he was sentenced to two years of probation and fined \$5,000.²⁶ Hacking by teens occurred as early as 1983 when six teens in Milwaukee area were accused of breaking 60 computer systems.²⁷ Many of the masterminds behind criminal acts are merely children who no longer need to be highly skilled to commit cyber crimes (What Is cyber Crime, 2003). The so-called hacker tools can be easily downloaded and employed by novice computer users. Some children might find themselves hanging out with skilled hackers who share hacking tools with them and encourage them to be destructive online. Children or teens may commit cyber crimes without realizing what they may consider a prank actually is a crime. Shutting down Web sites or releasing virus over the network is never an amusing prank but a serious crime. To make the matter worse, some parents might take pride in their children's savvy technical skills they cause interruption or destruction of computer systems.

Computer crime can be generally categorized into three types (What Is Cyber Crime, 2003). First, the computer is used as a target, such as attacking computers of others. One example is spreading viruses. Second, the computer is used as a weapon to commit crime that is seen in this physical world, for example, committing online fraud or operating online gamble. Third, the computer is used as an accessory, a filing cabinet, to store illegal or stolen information. Since going online becomes a favorite pastime for millions of children, the Internet becomes a convenient tool for them to find fun things to do though some fun things may turn illegal. The Internet may also become a fertile land for marketers to launch advertisement and entice children in purchasing products or revealing personal information. No

24 L. Lange, "Corporate America : Beware inside job," *Electronic Engineering Times*, 884(1996) : 20-21.

25 J. Chu, "Enemy at the gates?" *Time Atlantic*, 160 (2002) : 46-47.

26 B. Koemer, "Only you can prevent computer intrusions," *U. S. News & World Report*, 127 (1999) : 50.

doubt, numerous children profit from educational Web sites and powerful communication means. Nevertheless, they must remember that the Internet can harm them or others if children do not observe safe and responsible guidelines on the Internet.

What School and Parents Can Do

Today, resources for students are not limited only to print and non-print. To be information literate, students must be equally capable of accessing, using, and evaluating electronic resources and online databases for completing class work or pursuing personal interest. Numerous schools across the nation have installed filtering systems to keep inappropriate Web sites away from children. However, technology is not foolproof. Blocking technologies sometimes filter out useful information, and allow harmful materials to go through. Many schools have also established acceptable use policy (AUP) to ensure students' ethical and responsible behaviors on the Internet. AUP, served as an agreement among student, parent, and school, describes acceptable online behaviors for student use of computer equipment and the possible loss or suspension of privileges, if students are found violating the agreement. AUP stresses that use of school Internet is a privilege, not a right.

Schools may have filtering systems installed and AUP written, however, teachers still must instill in students the concepts of online safety and responsibility. Students need direction and guidance for their behaviors in the cyberspace as they do in this physical world. Internet safety and computer ethics should be integrated into classroom instruction. Schools have taught children various types of safety lessons, such as fire safety, tornado safety, laboratory safety, and traffic safety, so teachers can also include online safety as part of their instruction. Students need to know age appropriate ethics and legal issues regarding Internet use before they are allowed on the Internet.²⁸ It is beneficial for students to have class discussion on pirating software and prison sentences for illegally accessing another person's computer. In Cincinnati County Day School, every student in the 5th grade is issued a laptop. As students are permitted to use their laptops to access the school's network and the Internet, they spend one class period a day to study appropriate Internet behavior.²⁹ This school places strong emphasis on online safety and computer ethics. Generally, taking a couple of hours to address the topic probably would not make much impact on student online behaviors.

27 *Op. Cit.*, Komando.

28 L. MacVittie, "The rant," *Network Computing*, 13 (2002) : 32.

29 M. J. Zuckerman, & W. Rodger, "Linking online kids with real-world ethics education may be the way to head off young hackers," *USA Today*, (March 16, 2000), p. 1D.

Parents play an equally important role in educating and monitoring their children's online behaviors. After all, a majority of children spend more time navigating the Internet at home than at school. The Cybercitizenship Awareness Program, which is designed to educate children and teens on the dangers and consequences of cyber crime, suggests four approaches for parents to ensure their children's safe and ethical behaviors online.³⁰ First, parents must have a basic understanding of the technology. Second, parents participate with their children online. Third, parents determine what standards have been established for in-school computer use. Fourth, parents establish with their children a set of rules that clearly spell out parents' expectations relating to both ethics and safety. The ground rules for Internet access should include where, when, and which resources for children to access.³¹

It is essential to give students guidelines at home before they are allowed to go on the information highway. Parents as well as teachers must reiterate the concept of online safety and ethics, and frequently caution children never to reveal personal and family information to strangers. In addition, parents must encourage their children to share online experience with them, including both enriching and uncomfortable ones, and maintain an open communication with children concerning their online experiences. Most importantly, parents need to supervise their children's online behaviors and work alongside with schools in preparing children to cope with the Internet responsibility and freedom that they never experience.

Appendix

A. The Ten Commandments of Computer Ethics

1. Thou shall not use a computer to harm other people.
2. Thou shall not interfere with other people's computer work.
3. Thou shall not snoop around in other people's computer files.
4. Thou shall not use a computer to steal.
5. Thou shall not use a computer to bear false witness.
6. Thou shall not copy or use proprietary software for which you have not paid.
7. Thou shall not use other people's computer resources without authorization or proper compensation.
8. Thou shall not appropriate other people's intellectual output.
9. Thou shall think social consequences of the program you are writing or the system you are designing.

30 "Teaching cyber ethics," (2003). [Online] Available : <http://www.cybercitizenship.org/teaching>.

31 *Op. Cit.*, Teicher.

10. Thou shall always use a computer in ways that insure consideration and respect for your fellow humans.

(From Computer Ethics Institute<http://www.brook.edu/dybdocroot/its/cei/overview/Ten_Commanments_of_Computer_Ethics.htm>)

B Top Ten Netiquette Tips

10. Avoid using inappropriate and offensive language. There are so many other words to choose from!
9. Remember that nothing you write on the Internet is private. Anything written on the Net can be read by anyone online.
8. Avoid sending the same messages to the same people over and over again. This is called a pest.
7. Be cautious when using sarcasm or humor-people won't always get it! Try using emotions (smileys) when you want to be funny. :)
6. Avoid using All Caps. It's considered shouting online.
5. Avoid "Flames". These are useless messages that only hurt people's feelings.
4. Be concise. E-mail and chat sessions will be more productive if you keep your messages short.
3. Avoid spamming. It's like sending a batch of annoying junk mail.
2. Always delete unknown e-mail attachments before opening them. They can contain destructive viruses.
1. Only use you Member Name and/or e-mail address when chatting or sending e-mail. Never give out personal info like your name, address, phone number, or password.

(From CyberNetiquette.disney.com <<http://disney.go.com/cybersafety>>)