Internet Safety and Responsibility
Grades: 4 and 5
Emphasis: Cyber Bullying

	Fourth Grade	Fifth Grade

Cyber Community	I. Compare with the students their neighborhood community to the Cyberspace community.
	
	II. Review citizenship and safety with the students in the community by obeying laws and rules.
	
	III. What are the appropriate and inappropriate places to visit in both communities?
	
	IV. Compare "addresses" for locating places in both communities (street address and URL).
	
	V. Review the duties for being a responsible Cyber citizen.
	
	    A. Report inappropriate Web sites to an adult.
	
	    B. Use e-mail appropriately for communication with friends and family.
	
	    C. Never send threatening or mean e-mails, hoaxes, scams and SPAM.
	
	    D. Don't open e-mail from people you don't know.
	
	    E. Ask for permission to open email from your parents or teacher.
	
	    F. Never reply to SPAM.
		I. What are the features of a neighborhood physical community?
		
		    A. A community is a placed that is identified by address (restaurants, schools, stores, public libraries, etc.).
		
		    B. A community is a group of people who enjoy the same things, or engage in the same activities, such as a club, team, or school.
		
		    C. Make a list of safe places to go in the physical community.
		
		    E. List places that would not be safe to go in the physical community.
		
		II. What are the features of a cyber community?
		
		    A. The cyber community is made up of Web sites in which real people interact through electronic means.
		
		    B. Where is it safe to go?
		
		    C. Where would be inappropriate to go?
		
		III. What are some safety tips for traveling in cyber space?
		
		    A. Notify an adult about inappropriate Web sites.
		
		    B. Close the Web site with the X in the upper right hand corner.
		
		    C. For looping Web sites you may need to

		turn the computer completely off
Personal Safety	I. Discuss FBI Internet Safety Tips. (see poster attachment) II. Sometimes strangers lie about who they are, how old they are, what their names are and where they live when communicating on the Internet. III. Beware of e-mails that promise a surprise if you reply to their e-mail. IV. Identify what is considered personal information that is to never be given out to a stranger. (Name, age, phone number, address, zip code, school name, friend's or family names, or an information that can tell where you can be found) V. Never send your picture to a stranger. VI. Never write to someone who has made you feel uncomfortable, even if your parents know who it is. VII. Never meet someone you have talked with on the Internet or have them visit you without your parent's permission. VIII.Remember that people online may not be who they say they are. IX. When using Instant Messaging, stick to your "Buddy List" and use an unidentifying screen name. Make sure your parent know who the people are on your "buddy List." X. Chat rooms are programs where people talk by typing in their messages. Lots of people can look at the messages at the same time, and everyone can see everything that each person types. Private chats can be arranged. Beware of private chats.	I. There are various modes of communication. A. E-mail allows for communicating with an individual electronically. The person receiving the email will read and respond to the email in their on time. B. Instant Messaging allows 2 or more people to have a live conversation. Only the people allowed by the user are included in the conversation. C. Chat rooms are open live conversations usually on a subject of interest to all. Persons participating can see what everyone is saying and can join in when they want. II. Discuss why a stranger might try to contact you. III. How can they get your contact information? IV. Make passwords a combination of numbers and letters so it is not easy to guess. V. Discuss with the students tips for safety when communicating on the Internet A. Never tell anyone online personal information about yourself. The list below is a suggestion for what should not be made public. ● Your name or family name ● Your friends name ● Address ● Phone number ● Age ● Gender ● School ● Send your pictures B. E-mail is a formal means of communication and the e-mail address should represent who you are

| | XI. Bulletin boards are somewhat like chat rooms, except that the messages stay on the Web page for a long time for people to read. | (ex. jsmith@domain.com or editor@domain.org)

C. Chat rooms and Instant Messengers

    1. Choose a screen name that does not describe your identity.

    2. Select a unique password.

    3. Do not reveal any personal information.

    4. Understand the rules and consequences of inappropriate use of Internet communication.

    (See "Screen Name Activity" available from i-SAFE which is attached)

VI. Discuss the "Safety 4 R's" from i-SAFE America, Inc. (see attached poster)

    A. **RECOGNIZE** techniques used by online predators to groom.

    B. **REFUSE** all requests for personal information, to keep the relationship secret, or to meet anywhere.

    C. **RESPOND** assertively. Logoff, exit the program, or turn off the computer.

    D. **REPORT** suspicious or dangerous contact that makes you feel uncomfortable.

VII. What are the characteristics of how to identify a predator?

    A. Some people lie about who they are and what they want on the Internet.

    B. A predator is someone who victimizes somebody else.

    C. A predator uses lies, secrecy or stealth to get close enough to another to harm them. |
|---|---|---|

		D. An Internet predator preys on online users. E. Predators use the GROOM Process on their prey to gain their trust. F. They pretend to like the same things as you. G. They pretend to share your interests. H. They tell you they truly care about you. I. They always take your side against your parents. J. They want to become your new best friend. K. They always want to meet you.

Cyber Security	I. Explain about computer viruses like a worm or Trojan horse.
	
	II. How can your get a virus in your computer
	
	    A. Viruses can be hidden in an e-mail.
	
	    B. Viruses can be sent as an e-mail attachment.
	
	    C. If you see FWD: on the subject line of your e-mail this could mean could be a clue to a hidden virus.
	
	    D. Some viruses automatically forward themselves through all of the email addresses in your address book.
	
	III. The laws and rules punish the sender of a computer virus on purpose.
	
	IV. How do you prevent computer viruses?
	
	    A. Ask an adult before opening an e-
		I. Discuss e-mail etiquette. (Netiquette)
		
		    A. Flaming is sending a mean or hurtful e-mail.
		
		    B. Spamming is sending junk mail like jokes, hoaxes, urban legends, etc. to many people all at one time.
		
		    C. Forwarding is sending someone's personal information on to someone else.
		
		    D. Phishing is an email that is sent pretending to be from a real business that asks for personal information.
		
		II. What are malicious programs?
		
		    A. Malware are programs that include malicious code intended to harm, destroy or annoy. (virus, worm, Trojan Horse)
		
		    B. Listed below are safety tips for protecting

	mail. B. Don't open an attachment from someone you do not know. C. In chat rooms and instant messengers, only talk to people you know.	your computer 1. Install a firewall program on your computer. 2. Keep your computer updated with antivirus software as well as other software on your computer. 3. Don't open e-mails if you don't know who it is from. 4. Do not open attachments that have a suffix of ".exe", ".scr". or ".vsb". 5. Scan attachments with antivirus software.

Cyber Bullying	I. Discuss the difference between being kind and bullying.
	         A. Flame Mail is being rude.
	
	         B. Hate Mail shows racism, sexism and other prejudices.
	
	         C. Bulletin Boards are available on many subjects. Make sure you are sticking to the topic and that you comments are kind.
	
	         D. Chat sites are often monitored.
	
	         E. Stay away from Web sites devoted to making a person feel bad.
	
	II. Review e-mail netiquette (see attached poster)
	         A. Use a meaningful subject line. It should describe the content of the e-mail message.
	
	         B. Don't type with all CAPS that is just like screaming and is hard to read.
	
	         C. Think before you type, don't respond when upset.
		I. Discuss "kind" acts and "bullying" acts.
		
		II. Review Netiquette for e-mail, chat rooms and instant messengers.
		
		III. What are some tips for preventing cyber bullying?
		
		         A. Don't reveal your password, not even to your best friend.
		
		         B. Remember instant messaging conversations are not private. They can be printed, copied, forwarded, etc.
		
		         C. Be aware that pictures, video, and comments revealed online are not private. They can be shared with others without permission.

	D. Don't send large attachments in e-mail. E. Don't use email to spam by sending unwanted messages. F. Don't pass around chain letters.	
Intellectual Property	I. What are properties of the mind for both print and online formats A. Pictures that came from the imagination of the artist. B. The text of a book is the property of the person's imagination who created it. C. Magazine pictures, text advertisements, creative thought are all considered intellectual property. D. There are many more examples that can be used. See the definition in the vocabulary list included. II. You must site information or images that you use from the Internet.	I. Downloading music, movies or software from a legal site and paying for it does not permit you to make copies for your friends. II. Avoid plagiarism by citing the resources you use from the Internet. III. WCSD Bibliographic format can be found in the WCSD style manual. IV. Show students how to use Web based programs that are available for helping to create correct bibliographic citations.

Vocabulary

acronyms	**a word formed from the beginning letter or letters of each or most of the parts of a compound term** (Ex. HTML – Hyper Text Markup Language)
address book	**a feature of the email software that you use that allows you to store personal information including the e-mail address of an individual or group**
adware	any application that displays ad banners or serves ads to your browser (Companies pay people to spam you and these ads. Many offer free downloads to lure you to their site.)
attachments	**files attached to an email** (It can be a document, a picture, or a program.)
blog	**a Web site that contains an online personal journal with reflections, comments, and often hyperlinks provided by the writer**
bulletin board	**a public electronic forum that allows users to post or read messages or to post or download files and that is accessed by computer over a network (as the Internet)**
chat room	**a real-time online interactive discussion group**
citizen	**an inhabitant of a city or town; *especially* : one entitled to the rights and privileges of a freeman**
code	**a set of instructions for a computer**
communicate	**to convey knowledge of or information about**
community	**a group of people with a common characteristic or interest living together within a larger society**
copyright	**legal protection provided by the laws of the United States to the creators of things – like books, or other written work, as well as other dramatic musical and artistic works** (Copyright works must be tangible and are protected from being copied, distributed, and performed or changes without the creator's (or owner's) permission. This protection is available to published and unpublished works. In today's world, the Internet allows us easy access to ideas, creations, programs, etc., making Intellectual Property easy to steal. When you purchase music, movies, or software – you have purchased the right to use or listen to it – NOT to make copies for your friends. Remember, copying and distributing is a violation of copyright laws, not plagiarism. Don't copy illegally – it's stealing.)

cyber bullying	**those people who are bullies who use the Internet to knock others down** (E-mail provides one method of communication for these bullies. Flame mail – mail designed to make another person mad – is used along with hate mail – that shows racism, sexism, or other prejudices. Another way bullies use the Internet is through bulletin boards and chat sites to make their comments public. Some cyber bullies build Websites devoted to making a person or persons feel bad.)
cybercitizen	**an active participant in the online community of the Internet**
cyber community	**a community of Web pages and links that attract people with common characteristics and interests that can communicate with each other through digital communication** (Ex. email, chat rooms, blogs, bulletin boards, etc.)
cyber grooming	**the process that online predators use to trick their victims by building false trust and relationships**
cyberspace	**the online world of computer networks and especially the Internet**
e-mail	**a means or system for transmitting messages electronically**
emoticon	**is a word used for emotion icons** (When e-mailing, Instant Messaging, or chatting, writers use emoticons to show when they are joking, upset, or angry. Emoticons help the reading understand what the writer is really trying to say. Use characters on your keyboard to make emoticons. The most common one is the smile **: -)**. It is used to tell people – don't take what I said seriously; I meant it as a joke or in good humor.
fake subjects	**spammers fake the subject line of the e-mail so it looks like it could be from a friend** (Ex. "Re: your mail" – "Re: Hey" – "Re: Check this out!" – "Fw: u need to see this")
file extension	**a string of letters located at the end of a file name that explains the purpose of a file** (For example, hello.doc - .doc is the file extension. It explains the file is a document. .exe is an executable file – meaning it does something. .SCR stands for script and .vbs stands for visual basic, which is a programming language.)
firewall	**a filter used to block predetermined spam** (Screening methods include predetermined domain names or IP addresses.)
flaming	**is when you send a mean or hurtful e-mail** (Flaming tends to happen frequently on the net because it's easy to write things without thinking them through.)
flood	**an overwhelming quantity or volume of e-mail**

forward	**refers to sending to others an e-mail that you received from someone else** (When you forward e-mail, you are giving out personal information such as the e-mail address of the person who sent it to you. Forwarding e-mail can also be considered spamming. Make sure that e-mail you send has a point. If you have to forward something-forward it to yourself and BCC: the people you want to also receive it. This gives them the body of the message without all the other personal information.)
hacking	**the process of breaking into a computer or network** (This type of offense is criminal, and hackers will be prosecuted.)
hoaxes & scams	**stories, rumors, and urban legends circulating about the Internet** (Realize that not everything you receive in e-mail is true. Some examples are the e-mails that tell you to forward to ten friends and you'll receive money/gift certificates from a favorite store. Another harmful example is the e-mail that claims a virus may have been installed on your computer and you should delete a certain file. Often this file is a necessary one for your computer. Make sure you delete these types of hoax e-mails and don't pass them on.)
identity theft	**when someone uses your personal information to steal your identity for illegal purposes** (Ex. Social Security Number, credit card number)
instant message	**a form of real-time communication between two or more people based on typed text** (The text is conveyed via computers connected over a network such as the Internet.)
intellectual property	**a name used for material that is intangible** (You may not be able to touch it, but it does have value to the person who made it. (Examples: an idea, invention, expression or literary creation, unique name, business method, industrial process, chemical formula, computer program process, presentation, etc.)
Internet	**an electronic communications network that connects computer networks and organizational computer facilities around the world**
Internet Service Provider (ISP)	**the company from which you get your Internet service**
looping	**a Web design that does not allow you to leave the Web site when you click on the BACK button** (The Web site continues to comeback even though you want to leave the site. This is a sign that there may be danger at this Web site. Sometimes the only thing you can do is to turn off your computer.)
lurk	**to read messages on an Internet discussion forum (as a newsgroup or chat room) without contributing**
malicious code	programs written for a bad or destructive purpose.

malware	**another name for Spyware and Adware** (There are many ways to get malware on your computer. One way is to download an item with malware bundled into it. These types of programs are annoying and dangerous. They can send information to others about what you are doing online, sending pop-up advertisements to your screen, etc. In addition they can take up computer memory and cause frequent crashes. Be careful before ever downloading information of attachments.)
netiquette	**etiquette governing communication on the Internet**
newbie	**a newcomer to cyberspace**
online	**connected to, served by, or available through a system and especially a computer or telecommunications system (as the Internet)**
peer-to-peer (P2P) networks	**networks that make it possible for a user to download music, videos and games** (However, this is often STEALLING. You can be prosecuted if the artists and creators did not give permission for their works to be on the peer-to-peer network. In addition, downloading from these networks can carry other risks or penalties, such as viruses, adware and spyware that infect your computer. Legitimate peer-to-peer sites charge monthly fees or a per download fee so that they can pay the creator on you behalf – and you won't risk infection from malware or viruses.)
phishing	**using a business name without permission to send an e-mail asking for personal information** (You should never reply to these types of emails. They are usually from people trying to steal your information for illegal reasons. They are "fishing" for information – thus the term phishing.)
piracy	**when music, movies, and software is copied and burned illegally**
plagiarism	**occurs when you use someone else's work and pretend it is yours** (That includes when you "cut and paste" information or images from the Internet. Not only is it cheating, it is stealing. Also, even when you can use a picture for a school project under "Fair Use" laws, that does not mean you can claim credit for it. Consequences: fail the class, fail the assignment, suspension or expulsion from school, could affect college eligibility, lose you job, or get sued in court.)
posting	**publishing information to the Internet**
predator	**one that preys, destroys, or devours**
screen name	**a fake name that is used to identify you when you are in chat rooms, Instant Messaging, bulletin boards, etc.** (Screen names should not give away your gender, interests or any part of your real name.)
spam	**to send out a mass e-mail which is unwanted by the receiver of the e-mail**
spim	**to send out mass Instant Messages**

spoofing	**spammers fake the FROM line to fool the person receiving the e-mail as to who is really sending the e-mail** (At first glance everything looks legitimate – maybe from a family member or your ISP – but when you open it… you either are shocked by the content or it could contain a virus.)
spyware	**also known as trackware or thiefware, it uses your Internet connection to secretly transmit data to the company supplying the ads** (This data, including personal information required to install software on your CPU combines with information about you online activity, is then sold or traded to others. It's a sneaky way companies learn about their customers. It's also a violation of your privacy.)
steganography	**also known as <u>stego</u> - is a technology that allows people to embed or hide data inside of other files like documents (.doc) , pictures (.gif, bmp, jpeg) or music files (.wav, mpeg)** (The real message is hidden. It is believed that terrorists, drug traffickers, corporate raiders, and hackers use this way to communicate secretly. It is for this reason you shouldn't forward messages. You never know what the message really says and if it is altered, your name will be on it.)
Trojan horse	**computer programs that claim to do one thing, such as a game, but when run, secretly do other things such as to erase your hard drive** (These programs cannot replicate themselves. They have to be sent or copied by a user. A Trojan Horse program allows the designer a "back door" into their computer. This meant they could they could easily do what they wanted without the user ever knowing it. The only way to prevent getting a Trojan Horse virus is to only download from reputable sites.)
URL (Web site address)	acronym for Uniform Resource Locator - the address that is used to locate a Web site on the Internet
virus	**a computer program, which operates by piggybacking on other programs** (Any time the other program is run, the virus is activated and is able to do harm. When infected with a virus, email addresses can replicate themselves and send emails to anyone on your address list. Viruses can also spread if using an "infected" floppy disc in a computer.)
Website	**several Web pages on the Internet linked together and posted by the same person or organization**
worms	**viruses that spread through computer networks** (They use the network to replicate from machine to machine.)

Resources

Web sites
FBI Safety Tips: http://www.fbi.gov/kids/k5th/safety2.htm

iSAFE Series

NoodleTools

WCSD Style Manual