Internet Safety and Responsibility
Grades: 9-12

Cyber Community	I. Discuss the differences in the physical community and the cyber community. II. Listed below are guidelines for evaluating the best places to visit in the cyber community. A. **Information Websites:** Web sites you use to gain knowledge about something – the purpose is to present factual informational. The URL Address of these sites frequently ends in .edu (sponsored by educational institutions) or .gov (sponsored by government agencies). B. **Advocacy Websites:** Websites sponsored by an organization attempting to influence public opinion (that is, one trying to sell ideas). The URL address of this type of site frequently ends in .org (organization). C. **Business or Marketing Website:** Websites sponsored by a commercial business (usually trying to promote or sell products). The URL address of this type of site frequently ends in .com (commercial). D. **News Websites:** Websites designed to provide extremely current information. The URL address of this type of site usually ends in .com (commercial). E. **Entertainment Websites:** Websites that provide entertainment such as games, puzzles, or music. (Check these out carefully! Although many are created solely for the visitor's entertainment, a website of this type may actually be created to try to sell you an idea (Advocacy) or a product (Business), or to try to trick you into engaging in illegal or dangerous activity.) III. Develop evaluation criteria for individual Web sites to decide which the best are for you. A. Locate the author's name and qualifications B. Who is the publisher or sponsor? C. Locate the contact information. D. What is the date the Web site was created or updated. E. Can the information on the Website be proven in print resources? F. Is the page easy to use? G. Is the content relevance or understandable to age group? H. Is the content age appropriate?

	I. The Web site should not require you to provide personal information. J. Is the Web site free or subscription database? IV. What is the danger of pornography on the Web? A. Students and parents need to understand the potential effects of online pornography, and the relatively easy access to it, on children. B. Students and parents need to understand the basic laws surrounding pornography on the Internet and on the hard drive of your computer. C. Students and parents need to understand how the Internet pornography industry is exploiting youth.
Personal Safety	I. Stay safe when surfing the Internet, chatting, or e-mailing, by remembering to use the following guidelines. A. Never give out your first or last name, your parent's name, your home address, your phone number, birth date, etc. B. Don't tell anyone your password. C. Use discretion when giving out your screen name and user ID. II. To prevent SPAM use a different screen name from your e-mail address. View a Website's Privacy Policy to understand how they can use the information you give them. A. Ask for parental permission before giving out any personal information. B. You should be able to participate in most online activities without giving out personal information. C. Log off of a site if personal information is required. D. When you receive an e-mail that is inappropriate, delete it and report it. Don't ask to be removed, or click on the removal button. By doing that it informs Spammers that your address is a real e-mail address, and they will send more. E. Don't give out other people's names or e-mail addresses. You want to protect them, also. F. Don't register for contests or fill out information to download software. G. Understand that people aren't always who they claim to be. Don't give out information to

anyone claiming to be from the Internet Company, etc.

H. E-mail is not always private so don't put anything in there you would not want to see broadcasted.

III. Discuss cyber dating and cyber stalking.

IV. Newsgroups, forums, and bulletin boards can be a means by which a stalker can find out more information about a person.

A. Keep online interaction online. Don't agree to meet or phone people met online.

B. Don't give out personal information. Be careful about indirectly saying too much – like school mascot, game times, etc.

C. Keep your parents or guardians informed of online interaction.

D. Use Chat rooms that are moderated.

E. Be suspicious of someone who wants to be your friend and turns you against your parents, teachers or friends.

F. Private chats aren't always private – when you meet offline friends online in a private chat room be careful. Others can often enter and lurk.

G. Try to choose a gender-neutral online screen name.

V. How do spammers get your address?

A. By using software that creates thousands of made-up e-mail addresses, businesses can acquire e-mail addresses. A web beacon is placed in the spam e-mail that is sent to you. Every time an e-mail is opened, it is added to a live master list. The live list is then sold to other marketing and sales companies and the cycle never ends.

B. Companies scrape the web for e-mail addresses. Spammers look for Websites that list active e-mail addresses.

C. Registering for software on other products online is an easy way to hand over your e-mail address to be spammed. They usually tell you in the fine print.

D. Spammers buy e-mail addresses. It's a good chance that yours is one of them.

E. Be aware of fake subjects, spoofing, phishing, adware, spyware, firewalls and spim.

VI. Reporting Internet wrongdoing

A. **Call the local police and ask if they have a department with "Internet Crimes Against Children" (ICAC).**

B. **Simultaneously, file a report with the Cybertips Hotline at 1-800-843-5678.**

C. **Report the incident to the Cibertipline at** http://www.missingkids.com**.**

D. **If the incident was cyber stalking, report it** to your local provider and call the local police.

E. In the case of child luring, tell an adult, call the local police department. Notify the FBI and National Center for Missing and Exploited Children (NCMEC) 1-800-843-5678.

F. Report inappropriate material sent to a minor to NCMEC at 1-800-843-5678.

VII. Guide lines for how to identify a predator are listed below.

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 that you do.

G. They pretend to share your interests.

H. The predator tells you they truly care about you.

I. A predator always takes your side.

J. A predator wants to become your new best friend.

K. A predator always wants to meet you.

	VIII. Some techniques a predator uses are listed below A. They seek out provocative user names. B. They study your profile. C. It usually starts with an innocent Instant Message. D. They ask personal questions. E. They want you to talk with them in a private chat. F. They will start asking you for personal information. (Phone number, e-mail address, home address, school name, etc.) G. They want to be your best friend, boyfriend or girl friend. H. They start sexual conversations. I. The predator is all about keeping secrets. J. They will ask for personal photos. K. They might start to send you strange gifts. L. They want to set up a face-to-face meeting. M. They make threats when you no longer want to chat with them. IX. Ways to avoid predators are listed below. A. Recognize creepy techniques meant to deceive you. B. Choose safer user names C. Remove identifying information from your online profile. D. Set Chat boundaries on discussions (sex talk, problems you're having at home, school, etc.). E. Keep your personal information personal (school location, e-mail address, home address, phone number, cell number, hangouts, recent shows).

	F. IP Address – Static IP addresses can also be used to trace the location of your computer. Computers use IP addresses to locate and talk to each other on the Internet, much the same way people use phone numbers to locate and talk to one another on the telephone. A Static IP address is a number that is assigned to a computer by an Internet Service Provider (ISP) to be its permanent address on the Internet. Most ISPs use dynamic IP addresses, which means you are given a different IP address every time you log on and off the Internet. If your computer is left connected to the Internet, or if you operate on a wireless network that never shuts down, a person can find you by grabbing a satellite photo of the location of the IP address you are using. This is yet another reason why you should monitor your online communications. X. Listed below are criteria for reporting wrongdoings A. Save your emails. B. Take a screen shot of your chat room conversations. C. Write down all dates, times, and locations. D. Write down all nicknames, user names, and screen names. E. Create a history of your communications. F. Use your chat room quick response feature to report danger or harassment. G. Tell a friend. H. Tell a teacher. I. Don't log off. Keep your account open to show law enforcement. J. Contact the local polices and ask them if they have a department affiliated with "Internet Crimes Against Children" (ICAC). K. Contact your local policy department's cyber crimes unit. L. Report the incident to the Cybertip Hotline at 1-800-843-5678. M. Report the incident to the Cybertipline at http://www.missingkids.com.
Cyber Security	I. Malicious Programs can infiltrate your computer hard drive of network. A. Malware are programs that include malicious code intended to harm, destroy or annoy. (virus, worm, Trojan Horse) B. Safety Tips

	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. Guidelines for preventing cyber bullying are listed below. A. Tell someone. No one should put up with bullying! Don't keep it to yourself. Tell a trusted adult about the bullying. B. Don't open or read messages by cyber bullies. C. Tell you Internet Service Provider (ISP). D. Inform the local police. E. Tell your school if it is school related. Schools have a bullying plan in place. F. Don't erase the messages – they may be needed to take action. Instead put them in a folder unread. G. Stay protected and never agree to meet with a bully or with anyone, you meet online. H. If bullied through chat or instant messaging, the bully can often be blocked. II. Techniques for how to keep from being bullied online are listed below. A. Don't give out private information such as passwords, PINS, name, address, phone number, school name, or family and friends names. This information can be used by bullies and other harmful people on the Internet. B. Don't exchange pictures or give out email addresses to people you meet on the Internet. Ask permission from parents when it is necessary to give such information. C. Don't send a message when you are angry – it is hard to undo things that are said I anger. D. Delete messages from people you don't know, or those from people who seem angry or mean.

	E. When something doesn't seem right, it probably isn't. Get out of the site, chat, etc. III. What do you do if you are being bullied? A. Be strong and stop it early. Don't stoop to their level and lash back. B. Don't suffer in silence. Tell an adult. Keep telling people until someone takes action. C. Don't open or read messages from cyber bullies. D. Contact your ISP abuse department. E. If the problem continues alert the local police department. F. Tell your school if it is school related. If your cyber bully attends your school, contact your principal. G. Don't erase the messages. Log all dates and times. Put them in a folder and hold them as evidence. H. Change your email address or screen name. I. If it's happening with text messages, change your cell number. J. Take screen shots of your chat room pages. K. Save URLs, email addresses, and profiles of the bully. L. Stay protected and never agree to meet with a bully face to face. M. Block the bully if you are in a chat room or instant messaging.
Intellectual Property	I. Discuss what Intellectual Property is. II. U.S. Copyright Law {Title 17 U.S.C. Section 101 et seq., Title 18 U.S.C. Section 2319} protects copyright owners from the unauthorized reproduction, adaptation, or distribution of sound and video recordings, as well as certain digital performances to the public. Basically, it is illegal to steal the creative work of others and claim it as your own. III. Downloading music and movies without paying on unsanctioned sites is illegal and can result in criminal penalties. A. There is a good possibility of downloading viruses when you use a peer-to-peer site. B. You are creating a gateway for a hacker to break into your computer and steal your personal information. IV. To properly cite a source, use the bibliographic format as found in the WCSD style manual.

	V. Have students use Web based bibliographic citation generators which are free or require a subscription.
Personal Safety Web Space (My Space and other sites on the Web for placing personal information)	I. Post an anonymous e-mail address on the site. II. Make up a nickname and stick to it while posting. III. Keep posting fairly anonymous or unidentifying. IV. If you really want pictures on your site, password protect your site to only people you want to have access. V. If you really must blog on personal topics, password protect your blog. VI. Keep webcam use to family phone calls or personal friend interactions. Don't post them online for anyone to access. VII. If your friends know you personally, they should already know your Instant Messaging screen name. Anyone who asks for it online could be dangerous. VIII. Keep your family informed as you meet people online or get e-mails. Setup ground rules in advance.

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 stego - 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

i-SAFE Series

i-SAFE Web site: http://www.isafe.org

NoodleTools

WCSD Style Manual

Call the Cybertips hotline at 1-800-843-5678

Cybertip Website at http://www.missingkids.com

http://www.ciac.org