Internet Safety and Responsibility
Grades: 6, 7, & 8
Emphasis: Predator identification and cyber community citizenship

	Sixth Grade	Seventh Grade	Eighth Grade
Cyber Community	I. Community is the physical area where we live, comprised of places where we know and interact with real people. II. Community is also a group of people who enjoy the same things, or engage in the same activities, such as clubs, teams, or school. III. Cyberspace is also a community made up of Web sites to visit and people who have similar interests.	I. Listed here are features of the neighborhood physical community. A. A community has places that are identified by an address like 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. List safe places for students to go in the community. II. Features of the cyber community are as listed below. A. The cyber community contains Web sites in which real people interact through electronic means. B. Where is it safe to go? C. Where would it be inappropriate to go? (Sites that ask for money for any reason, sites that ask for your personal information such as name and e-mail address, gambling sites, sites which contain R-rated or X-rated pictures or words not appropriate for kids, and sites which tell about	I. Discuss the differences in the physical community and the cyber community. II. Use the following guideline 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

		violence or hate toward other people.) III. Safety tips are listed below for traveling in cyber space. A. Notify an adult about inappropriate Web sites. B. Close inappropriate Web sites with the X in the upper right hand corner. C. For looping Web sites you will need to turn the computer completely off.	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 Websites to decide which the best are for you. A. Identify the author's name and qualifications.

			B. Who is the publisher or sponsor? C. Locate contact information. D. Find the date created or updated of the Web site. E. Can the information on the Website be proven in print resources? F. Is the page easy to use? G. Is the information relevant or understandable to the age group intended? H. Does it have age appropriate content? I. The Web site should not require you to provide personal information. J. Is it a free Website or subscription database?

Personal Safety	I. Dangers that should concern Internet users are predators, people stealing money, bullying, inappropriate websites, and hate sites. II. Students should model good uses of the Internet, such as research, credible information, maps, and museums. III. Email safety guidelines are listed below. A. Never give out your phone numbers. B. Never give you're your address. C. Never tell your age. D. Never tell your gender. E. Never identify your family member's names. F. Never identify your school, mascot or team names. IV. Instant messenger and chat room safety tips are listed below. A. Choose a screen name that does not give away your identity and is gender neutral. B. Choose a unique	I. Various modes of communication available through Internet are e-mail, instant messaging, and chat rooms. A. Discuss why a stranger might try to contact you. B. How can they get your contact information? C. Make passwords a combination of numbers and letters so it is not easy to guess. II. Below are guidelines for safety when communicating on the Internet. A. Never tell anyone online your name or family name. B. Never tell anyone your friend's name. C. Never give out your address. D. Never give out your phone number. E. Never tell people you do not know that you met online your age. F. Do not indicate to online acquaintances your gender. G. Never let them know what school you attend. H. Never send your picture to someone you meet online.	I. When surfing the Internet, chatting, or e-mailing, stay safe by remembering the following tips. 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. Be careful of to who you tell your screen name and user ID. D. 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. E. Ask for parental permission before giving any information out. F. You should be able to participate in most online activities without giving out information. G. Log off if personal information is required.

	password. C. Do not give out any personal information. D. Think about what could happen when you are communicating. V. Safety tips for chats and instant messaging are listed below. A. Keep online interaction online. Do not agree to meet or phone people met online. B. Don't give out any personal information like school mascots or games times. C. Keep your parents or guardians informed of online interaction. D. Use only Chat rooms that are moderated. E. Be suspicious of anyone who tries to turn your parents, teachers or friends against you. F. Private chat rooms are not private. Others can LURK. VI. Report Internet wrong-doings through the following agencies.	III. Email is a formal means of communication and the e-mail address should represent who you are (ex. jsmith@domain.com or editor@domain.org). A. Many companies advertise via e-mail. They try to entice you to purchase items, visit inappropriate sites, etc. Delete their e-mails. B. Be careful when you reply to an e-mail. You are including your e-mail address and you don't know where it will go from there. C. Inappropriate, offensive, angry e-mail should be reported to your Internet provider. D. Remember the sender of an e-mail may not be someone you know-don't send personal information, photographs, etc. IV. Dangers is chat rooms and instant messengers are listed below 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	H. 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 – that informs Spammers that yours is a real e-mail address and they will send more! I. Don't give out other people's names or e-mail addresses- you want to protect them, also. J. Don't register for contests or fill out information to download software. K. 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. L. E-mail is not always private so don't put anything in there you would not want to see broadcasted. II. Discuss newsgroups, forums, and bulleting boards. A. Keep online interaction online. Don't agree to meet or phone

	A. Call local police ad ask for Internet Crimes Against Children (ICAC). B. Call the Cybertips hotline at 1-800-843-5678. C. Report the incident to the Cybertip Website at http://www.missingkids.com. VII. Below you will find 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. VIII. Below are guidelines to help identify a predator. A. Some people lie about who they are and	moderated. E. Be suspicious of someone who wants to be your friend and turns you against your parents, teachers or friends. F. Private chats are not 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. Dangers in newsgroups, forums, and bulletin boards are listed below. A. The biggest risk is in including personal information in postings. Don't reveal anything identifying about yourself. B. Realize that by posting, you are making your address public. C. Groups that are illegal or want to spread hateful messages may try to get you involved. VI. Safety 4 R's from i-SAFE America, Inc. are listed below. (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.	people met online. B. Don't give out personal information. Be careful about indirectly saying too much – like school mascot, game times, etc. Eventually you will have said enough. 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. III. Guidelines for reporting Internet wrongdoing. A. Call the local police and ask if they have a department with

	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. G. They pretend to share your interests. H. They tell you they truly care about you. I. They always take your side. J. They want to become your new best friend. K. They always want to meet you.	C. **RESPOND** assertively. Logoff, exit the program, or turn off the computer. D. **REPORT** suspicious or dangerous contact that makes you feel uncomfortable. VII. Following are guidelines for how to identify a predator. A. Some people lie about who they are and what they want on the Internet. B. 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 you do. G. They pretend to share your interests. H. They tell you they truly care about you. I. They always take your side in an argument or emotional situation.	"Internet Crimes Against Children" (ICAC). B. Simultaneously, fire a report with the Cybertips Hotline at 1-800-843-5678. C. Contact the Cibertipline at http://www.missingkids.com. D. Report cyber stalking to your local provider and call the local police. E. If the incident involves 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. If the event involves Inappropriate material sent to a minor, call NCMEC. IV. Below are guidelines for 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

		J. They want to become your new best friend. K. They always want to meet you. VIII. Guidelines for reporting incidents are listed below. A. Call the local police and ask if they have a department affiliated with “Internet Crimes Against Children” (ICAC). B. Contact the Cybertip Hotline at 1-800-843-5678. C. Report the incident Cybertipline –at http://www.missingkids.com	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. Predators pretend to like the same things. G. Predators pretend to share your interests. H. Predators tell you they truly care about you. I. Predators always take your side. J. Predators want to become your new best friend. K. Predators always want to meet you. L. V. Listed below are guidelines for reporting incidents. A. Call the local police and ask if they have a department affiliated with “Internet Crimes

			Against Children" (ICAC). B. Report the incident to the Cybertip Hotline – 1-800-843-5678. C. Contact the Cybertipline at http://www.missingkids.com.
Cyber Security	I. E-mail security problems come in the form of flaming, spamming, forwarding and hoaxes. II. Malicious Programs come in the form of Malware, viruses, worms, and Trojan Horses. III. Ways to get a virus are listed below. A. Viruses can be hidden in an e-mail. B. A virus can be part of an e-mail attachment. C. FWD: means email has been forwarded. This could be a clue to a hidden virus that automatically forwards a malicious virus. D. Some viruses automatically forward themselves through all of	I. Avoid the following when working with e-mail. A. Flaming – the sending of a mean or hurtful e-mail. B. Spamming - sending junk mail like jokes, hoaxes, urban legends, etc. to many people all at one time. C. Forwarding - sending someone's personal information on to someone else. D. Phishing – an email that is sent pretending to be from a real business that asks for personal information. E. Malware – programs that include malicious code intended to harm, destroy or annoy (virus, worm, Trojan Horse). II. Safety tip guidelines are listed below. A. Install a firewall program on your computer.	I. Malware are programs that include malicious code intended to harm, destroy or annoy. (virus, worm, Trojan Horse) II. Safety tips guidelines are listed below. A. Install a firewall program on your computer. B. Keep your computer updated with antivirus software as well as other software on your computer. C. Don't open e-mails if you don't know who it is from. D. Do not open attachments that have a suffix of ".exe", ".scr". or ".vsb". E. Scan attachments with antivirus software.

	the email addresses in your address book. IV. Laws and rules to punish the sender of a computer virus on purpose are in place. V. Ways to prevent viruses from damaging you computer. A. Ask an adult before opening an e-mail. B. Don't open an attachment from someone you do not know. C. When using chat rooms and instant messengers, only talk to people you know.	B. Keep your computer updated with antivirus software as well as other software on your computer. C. Don't open e-mails if you don't know who it is from. D. Do not open attachments that have a suffix of ".exe", ".scr". or ".vsb". E. Scan attachments with antivirus software.	
Cyber Bullying	I. Discuss the difference between being kind and bullying. II. Listed below are examples of bullying using e-mail. A. Flame mail is the term used for being rude in an e-mail message. B. Hate mail is the term used for showing racism, sexism and other prejudices in an e-mail message. III. Bulletin boards are public postings that can be read by anyone and do not go away. If used for hurting someone or a group this is a form of 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.	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

	IV. Chat sites are live conversations with a group of people where everyone can see what the conversations are and join in at any time. Bullying can occur on chat sites. Students should use moderated chat rooms. V. Websites devoted to making a person feel bad are a form of bullying. VI. Protect yourself from cyber bullies by using the suggestions listed below. A. Don't open or read messages by cyber bullies. B. Tell your parents, teacher or principal if you should receive an e-mail that makes you feel uncomfortable. C. Don't erase the message. It may be needed for evidence by the police. D. Never agree to meet with the bully or any person you meet online. E. Block them from chat rooms or instant messaging. F. Call you ISP and	F. Don't erase the messages – they may be needed to take action. Instead put them in a folder unread. G. Stay protected – 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	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 – 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. IV. 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.

	report incident. G. If you are threatened with harm, inform your local police. VII. E-mail Netiquette guidelines are listed below. (see attached poster) A. Use a meaningful subject on the subject line to indicate to the reader what the e-mail content will be about. B. Don't type with all CAPITALS letters. In e-mail that is interpreted as screaming. C. Think before you type and don't respond when upset. Sometimes picking up the phone is a better way to respond. D. Use emoticons to convey your mood or intent. (Teachers, be careful as some of the lists of emoticons that you find on the Internet. Some are very inappropriate for students. Attached is a safe list of emoticon examples.) E. Using Internet acronyms in chat rooms and instant messaging can shorten the number of words that need to be	the site, chat, etc. III. Guidelines for preventing cyber bullying are listed below. I. Tell someone. No one should put up with bullying! Don't keep it to yourself. Tell a trusted adult about the bullying. J. Don't open or read messages by cyber bullies. K. Tell you Internet Service Provider (ISP). L. Inform the local police. M. Tell your school if it is school related. Schools have a bullying plan in place. N. Don't erase the messages – they may be needed to take action. Instead put them in a folder unread. O. Stay protected – never agree to meet with a bully or with anyone, you meet online. P. If bullied through chat or instant messaging, the bully can often be blocked. III. 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	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. V. 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

	typed. (Attached is a list of commonly used acronyms.) F. Don't send an attachment if it can be copy and pasted into e-mail. G. Don't send large attachments. Some e-mail providers only allow email of a certain size to be downloaded into a person account. H. Don't SPAM by send unwanted messages to other e-mail addresses. I. Don't pass around e-hoaxes. J. Don't pass around chain letters. K. Be nice to newbies in chat rooms and instant messaging.	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.	messages – they may be needed to take action. Instead put them in a folder unread. G. Stay protected – 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. VI. 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.
Intellectual Property	I. What are properties of the mind for both print and online formats? A. Pictures that have been created by the imagination of the originator. B. Book written with the imagination of the originator. C. Magazine articles, photographs, and advertisements that are the creation of the imagination of the originator. II. You must site information or images that you use from the Internet. III. Copyright and Fair Use apply to information taken from the Internet just like they do from print resources. IV. Plagiarism can be avoided by citing your sources and following the policies pf the WCSD.	I. Define Intellectual Property. II. Discuss copyright in relationship to the Internet. III. Discuss peer-to-peer networks. IV. WCSD Bibliographic format can be found in the WCSD style manual. V. Use free or subscription bibliographic generators to create bibliographic citations. VI. Review the WCSD District Internet Safety Policy (Acceptable Use Policy). VII. Review WCSD Policy about cell phones.	I. Define Intellectual Property. II. Discuss copyright in relationship to the Internet. III. Discuss peer-to-peer networks. IV. WCSD Bibliographic format can be found in the WCSD style manual. V. Use free or subscription bibliographic generators to create bibliographic citations. VI. Review the WCSD District Internet Safety Policy (Acceptable Use Policy). VII. Review WCSD Policy about cell phones.

	A. Review with the students the WCSD Internet Safety Policy. (Acceptable Use Policy) B. Review with the WCSD policy about cell phones. C. Show students how to use free or subscription Web based bibliographic citation generators.		
Personal Safety Web Space (My Space and other sites on the Web for placing personal information)	I. Post an anonymous e-mail when creating a Web site. II. Make up a nickname and stick to it while posting. III. Keep your 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		I. Post an anonymous e-mail when creating a Web site. II. Make up a nickname and stick to it while posting. III. Keep your 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.		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 <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.)