Cyber Smart Week for Grade 9 - 12
Introduction and Instructional Materials

Senate Bill 1492 requirements that schools, as part of their Internet safety policies, educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. To fulfill the requirements of SB 1492 as incorporated into the OUSD District Technology Plan (2011-2014) technology goals and benchmarks, OUSD is providing lesson materials to educate students and teachers on the appropriate and ethical use of information technology in the classroom, Internet safety, plagiarism, copyright, and the implications of illegal peer-to-peer network file sharing. The materials are to be used by OUSD classroom teachers during Cyber Smart Week.

Each day during Cyber Smart Week, teachers should plan to spend 10-15 minutes delivering information to students on the topic for that day.

**Daily Topics for Grades 9-12**
- Monday, – Identity Privacy and Social Networks
- Tuesday, – Online Protection and CyberPredators
- Wednesday, – Piracy, Copyright, and Plagiarism
- Thursday, – Netiquette, Acceptable Use, and CyberBullying
- Friday, – Check for Understanding

Teachers may deliver the information to students through reading the script provided for each day. Daily PowerPoint presentations are available for teachers who wish to use a computer to deliver the information. Each day’s information is accompanied by optional extension activities – Internet links to PDF worksheets, games and videos – which may be accessed, printed, and used in the classroom, library, or computer lab at the teacher’s discretion. A quiz to check for student understanding and an online survey for teachers to complete conclude the week’s activities.

The Cyber Smart Week information packet also includes a glossary of terms used in the instructional materials and a letter to parents in English and Spanish describing the week’s activities.

The parent letter, daily scripts, glossary, links to activities, daily PowerPoint presentations, quiz, and evaluation survey are posted on the OUSD website and can be found at http://www.ousd.k12.ca.us/cybersmart. All material may be accessed, downloaded, and reproduced for informational and instructional use only.

For answers to questions about these activities, please contact Ann Kruze, Coordinator of Instructional Technology (a Division of Leadership, Curriculum and Instruction) at ann.kruze@ousd.k12.ca.us.
Internet Safety and Privacy – Playing It Safe and Smart
Day 1: How to Use the Internet Safely: Identity Safety and Social Networks

Review:
The glossary in the packet if you are unfamiliar with the vocabulary terms in this lesson.

Introduce Cyber Smart Week to the students:
Say:
“This week we’re going to spend a little time every day discussing how to use computers and the Internet to become smarter and safer.”

Ask students:
“What are some things you like to do on the computer?”

Discuss:
The majority of students will have played games or visited websites at home or at school. Answers might also include Instant Messaging (IM’ing) or online chatting with friends, visiting social networking sites such as FaceBook or MySpace, checking or sending email. Some students may also write “Blog” entries. Most will also have used some applications such as Microsoft Office.

After getting student input on some of the possible activities that can be done on the computer, focus the discussion:
Say:
“The ability to interact and communicate with others is one of the things we enjoy the most about computers. Going to the Internet to find information, emailing friends, and other interactive activities make using computers fun and educational. The Internet is a new world full of interesting people and places that can benefit our lives. Just like the real world, however, the Internet world can be a dangerous place if we don’t know how to make safe and smart choices.

It’s very important that you involve your parents in your online activities, especially if your family shares a computer. Ask an adult for help if you have questions about things you find online.”

“Today we’ll talk about making smart choices to protect our personal information online. Why does this matter? - because the Internet makes it easy for websites to collect and store your personal information. When you answer online surveys, enter contests or fill out online registration forms, there are often questions designed to obtain personal information such as your email address, age, and other items. This might seem harmless, but marketers can use this information to send you or your family “junk email” or “spam”. Some of these websites are even worse. Some download programs onto your computer that you don’t want and that can prevent your computer from running correctly.”

“Some websites ask for more personal information like name, gender, age, home address, phone number, picture, credit card information or passwords. When you sign up for instant messaging software, for example, you are asked if you would like to fill out a personal profile. The fields include ‘real’ name and address as well as details about your personal life. Once completed, this profile is available to anyone on the Internet who wants to pull it up and read it. Even worse, others capture information that is later used for identity theft. Teenagers are often targeted for identity theft since they present a “clean slate” for identity thieves. That’s why it’s especially important that you protect your Social Security number.”

“FaceBook or MySpace are social networking websites where people can post a profile and communicate with others. This profile can be an example of “too much information” if it contains facts about your name, where you live or go to school, or other personal information. It can also be embarrassing if you have posted inappropriate pictures or other items to your profile since once it’s online, everyone can see it. These online profiles are being called “digital resumes” and employers and college admissions officers have been known to look at them to determine whether applicants are qualified. Think about it - would you want a future employer to see your MySpace page?”

Ask students:
“What are some smart privacy rules for CyberSpace?”
Discuss:

• Don’t fill out online forms or surveys or enter contests without parent permission.
• Don’t share personal information online such as name, address, phone number, age, gender, photo or Social Security number.
• Remember that everything you post to the Internet can be seen by anyone and everyone.

*If time allows, ask if students have any questions.

Resources and Activities:
Grade 9-12 - http://cybersmartcurriculum.org/safetysecurity/lessons/9-12/your_online_image/
CyberSmart!© activity with downloadable PDF student worksheet for discussing potential consequences of posting social networking information.

Online Activity:
Grades 9-12 Post-To-Be-Private (Online Video: English and Spanish)
http://www.nsteens.org/videos/social-networking/
Short video that presents information on creating a safe online profile with student activity cards for extension

Citation:
© 2008 Media Awareness Network, www.media-awareness.ca, adapted with permission
Internet Safety and Privacy – Playing It Safe and Smart
Day 2: Internet Safety: Online Protection and CyberPredators

Remind students about Cyber Smart Week:

Say:
“Remember that this week we’re going to spend a little time every day talking about using computers and the Internet to become smarter and safer.”
“Yesterday you learned some basic rules to protect your personal privacy while you enjoy the benefits of the Internet like finding information, playing games, and communicating with others. Let’s review the rules we discussed yesterday.”

Ask students:
“What Internet rules do you remember from yesterday?”

Discuss:
• Don’t fill out online forms or surveys or enter contests without parent permission.
• Don’t share personal information online such as name, address, phone number, age, gender, photo or Social Security number.
• Remember that everything you post to the Internet can be seen by anyone and everyone.

Say:
“Yesterday we briefly talked about the fact that when you put information about yourself on the Internet anyone can see it; and that really personal information like your name, age, where you live, phone number, and where you go to school should never be shared. There are many reasons why sharing this information on the Internet is a bad idea. The most serious reason for keeping your private information private, though, is that some adults try to take advantage of teenagers by pretending to be friends when they really have bad intentions. They try to get personal information like where you live or go to school by lying and deception. They are called “cyberpredators” or “online predators”.

“Cyberpredators try to meet teenagers through conversations in chat rooms, instant messaging, e-mail or discussion boards. They often lie about their age and pretend to be younger, often as young as the person they are trying to contact. Online predators try to make friends through attention, affection, kindness, and even gifts, and often devote considerable time, money and energy to this effort. They know about the latest music and hobbies likely to interest teens. They specialize in listening to and sympathize with young adult problems. They also try to ease young people’s inhibitions by gradually introducing overly personal content into their conversations or by asking for or sending inappropriate material. Some predators work faster than others, engaging in inappropriate conversations immediately. This more direct approach may include harassment or stalking. Predators may also evaluate the kids they meet online for future face-to-face contact.”

“You might think you’re too smart to fall for this. After all, you’re old enough to know not to talk to strangers or get into a car with someone you don’t know, right? And you probably believe that if even in online communication you can tell the difference between a potential friend and a bad adult. Well, consider this: cyberpredators are very patient. Some will maintain a false identity for weeks while they get their victims to trust them.”

“Some very smart kids have believed cyberpredators lies and become victims, so it’s best to remember some simple rules to avoid them:”

Discuss:
• Never give personal information to people you meet online including your real name and especially where you live – even little things can be used as clues by skilled searchers to find out where you live or go to school.
• Be alert for cyberpredators – people who try to gain your trust or ask inappropriate questions such as whether your parents are home.
• Never meet anyone in person who contacts you online without parent permission; even then, take a trusted adult with you.
• Never respond to online chat or email messages that make you feel uncomfortable – instead, tell an adult.
• If after telling an adult you continue to be bothered, have a trusted adult call the CyberTipline (http://cybertipline.com or 800-843-5678)

*If time allows, students might wish to ask questions, share personal experiences, or get clarification. Consider a class discussion at this point.

**Resources and Activities:**

Grades 9-12: Making Good Decisions
http://cybersmartcurriculum.org/safetysecurity/lessons/9-12/making_good_decisions/

CyberSmart!© Student activity for grades 9-12 with downloadable PDF student quiz to examine good choices high school students can make to avoid being exploited by Internet predators.

**Online Activity:**

Downloadable WMV Video File: Amy’s Choice/English and Spanish

**Citation:**

© 2008 Media Awareness Network, www.media-awareness.ca, adapted with permission
Digital Citizenship – Keeping It Ethical and Responsible
Day 3: Piracy, Copyright and Plagiarism

Remind students about Cyber Smart Week:
Say:
“Remember that this week we’re going to spend a little time every day talking about using computers and the Internet to become smarter and safer.”
“For the past two days we’ve talked about how to be safe when we use computers.”

Ask students:
“Who remembers what our Internet safety rules are?”

Discuss:
• Don’t fill out online forms or surveys or enter contests without parent permission.
• Don’t share personal information online such as name, address, phone number, age, gender, photo or Social Security number.
• Remember that everything you post to the Internet can be seen by anyone and everyone.
• Never give personal information to people you meet online including your real name and especially where you live.
• Be alert for cyberpredators – people who try to gain your trust or ask inappropriate questions such as whether your parents are home.
• Never meet anyone in person who contacts you online.
• Never respond to online chat or email messages that make you feel confused or uncomfortable – instead, tell an adult.
• If after telling an adult you continue to be bothered, have a trusted adult call the CyberTipline (http://cybertipline.com or 800-843-5678)

Say:
“Today I want to talk about how to be good citizens when we use computers and the Internet. You all know how to be good citizens – how to respect each other accept responsibility for your own behavior and its consequences. Well, we need to be good citizens in cyberspace too – we need to practice cyberethics.”

“When you create something original, aren't you proud of your work, especially when you spend a lot of time and energy creating it? A science report, a great drawing, a song or poem you wrote, or even the pictures you took on vacation can be a great source of personal accomplishment. All these are your own creations and you'd probably be pretty upset if someone just copied any of them without your permission - especially if they tried to pass them off as their own work and didn’t even give you credit. That's where copyright law comes in. Copyright law gives you a set of rights that prevents other people from copying your work or doing things with your work that you might not like without your permission.”

“As the creator of your own work, you have the right to control what people can and can’t do with it. Only you have the right to sell it if you want to. And just like you, the people who create screenplays for movies and television shows, books, computer games, webpages, music, and photography deserve to derive the benefits from the hard work they put into their creations. That's what copyright is all about. It reflects our respect for what we call “intellectual property” and the rights that go with that property.”

“So what happens when you copy a CD or a DVD you didn’t pay for or download copyrighted games or songs illegally from the Internet? You are guilty of “copyright infringement”. It’s actually against the law because it’s just like stealing. Think about it – if your favorite band can’t make money because no one is paying for their music but is copying it instead, they won’t be able to continue to work. Illegal downloading and copying is a big problem for creative artists because it deprives them of the right to make a living from their work. And if they can’t make a living, they might cease to create, and then we don’t get to enjoy what they do.”

“Copyright infringement is serious, but copying and then reselling copyrighted works like CD’s, games, and DVD’s is even worse – it’s criminal. It’s called “piracy” and when people are caught doing this, they can go to jail. We should avoid buying pirated material. Often it shows up at very low prices at places outside of established stores, like street markets. Although the low prices might be tempting, remember that pirated CD’s or DVD’s are not just bad for artists, they’re bad for consumers. There’s no protection against faulty copies so you could be wasting your money. Supporting piracy also makes legal copies more expensive for everyone because publishers and distributors must increase prices to recover these losses. So let’s state the first two cyberethics rules we’ll follow.”
Discuss:
- Respect intellectual property and copyright law.
- Only download with artist permission or from copyright-free Internet sites.

Say:
“Now what about school work?”

Ask students:
“Is it okay to copy and paste from the Internet or copy from books if it’s for a report or a presentation for school?”

Say:
“Of course not! There’s nothing wrong with taking an idea from a book or the Internet and making it original by expanding the concept and taking it in a new direction. But that doesn’t mean just changing a few words around – that’s not original.”

“Copying from books or cutting and pasting from the Internet and then trying to pass it off as your own work is a very bad idea. It’s called plagiarism. Schools, universities, and businesses have strict rules against it because it’s dishonest – it’s not just stealing, it’s lying about it too. When you plagiarize, you’re also cheating yourself out of the kind of authentic learning experience you need to be successful in college or on the job.”

“So, the next cyberethics rule is: Never plagiarize – keep your work original.”

Discuss: Plagiarism

Say:
“Sometimes though we like the way an author expresses an idea so much that we want to use their exact words in our own work and that’s fine. Just remember to copy the wording exactly and put “quotation marks” around it.

Quotation marks let whoever is reading our work know that this particular text is taken from another person’s work. Remember also to state where you got the quotation from – in other words, site your source. A citation gives the title and author or location on the Internet, and other information for the quote. Something else you should cite is information or ideas that you’ve taken directly from another author, even if you’ve put them in your own words.

You don’t need quotation marks for these, but you need to state where the information came from. This also applies to pictures or music downloaded from the Internet, even with permission. Your source still needs to be cited. So here’s our final rule: Always cite your sources.”

“So let’s review all four of our rules:”

Discuss:
- Respect intellectual property and copyright law.
- Only download with artist permission or from copyright-free Internet sites.
- Never plagiarize – keep your work original.
- Always cite your sources.

*If time allows, ask if students have any questions.

Resource and Activities:
Grades 9-12: Considering Copying
http://cybersmartcurriculum.org/mannersbullyingethics/lessons/6-8/considering_copying/

CyberSmart!© Student activity with downloadable PDF worksheet to examine copyright, fair use, plagiarism, and hacking.

Online Resources:
Grades 9-12: You Quote It, You Note It!
http://library.acadiau.ca/tutorials/plagiarism/

Online interactive tutorial that humorously explains plagiarism in depth.

Grades 9-12: CyberEthics for Kids Online Quiz - US. Dept. of Justice
http://www.cybercrime.gov/rules/kidinternet.htm

A variety of activities and resources including an interactive quiz on a variety of issues including legal and illegal downloading from the Internet.

Citation:
© 2007 The Copyright Society of the U.S.A., www.copyrightkids.org, adapted with permission

OUSD-Instructional Technology (LCI) Grades 9-12
Curriculum organized by Santa Ana USD
Digital Citizenship – Keeping It Ethical and Responsible
Day 4: Let’s Be Good CyberCitizens: Acceptable Use, Cyberbullying, Netiquette

Remind students about Cyber Smart Week:
Say:
“Remember that this week we’re going to spend a little time every day talking about using computers and
the Internet to become smarter and safer.”
“Let’s review the cybercitizenship rules we discussed yesterday.”
Ask students:
“Who can remember what they are?”
Discuss:
• Respect intellectual property and copyright law.
• Only download with artist permission or from copyright-free Internet sites.
• Never plagiarize – keep your work original.
• Always cite your sources.

Say:
“Today I want to talk more about how to be good citizens when we use computers and the Internet. So far this
week we’ve talked about responsibility. Think about it a minute. When we’ve discussed being careful about
not giving personal information online or being alert for cyberpredators, we’ve really been talking about
responsibility for taking good care of ourselves and our computers. We talked about rules for being good
cybercitizens too - like not copying from others or always giving credit when we use information. Obeying rules
is part of being responsible because when we all obey the same rules it makes it easier to learn together as a
community.”
Ask students:
“What do you think would happen if we didn’t all obey classroom rules but everybody just did whatever they
wanted whenever they wanted?”
Discuss:
Student responses – someone could be hurt, we wouldn’t get any work done, etc.
Say:
“Besides Cyber Smart rules, our schools have rules for using computers and the Internet. These were included
in an agreement you and your parents received in your registration packet. When you signed it, you agreed to
abide by the district’s rules for Acceptable Uses for Technology. You may not remember that, so let’s review
what you agreed to.”
“Some of the district rules are similar to our Cyber Smart rules: never share personal information, remember
that everything you put online can be seen by anyone, always cite your sources, and never copy from others.
Other rules are a little different. For example, students are responsible for taking good care of our school
computers. That means respecting the equipment and software and following computer lab, classroom, and
school rules. No one should download anything to school computers or install any software without
permission.”
“Students should also use the Internet responsibly. That means not using the Internet for promoting or posting
anything illegal or immoral; the network can’t be used for commercial purchases or for political advertising.
You also need to take good care of any passwords you might use to access software, email, or computer files.
Passwords should always be private and never shared with anyone, even your good friends.”
“One of the most important rules is that the Internet not be used to harass anyone. You might be wondering –
how could I be harassed by a computer? Well, unfortunately, some individuals have been known to use email
or social networking sites like MySpace or FaceBook to write unflattering, hurtful, or threatening things to or
about others. When kids are intentionally or repeatedly mean to each other in this way, it’s called
“cyberbullying”. If this happens to you, it’s important not to respond to the bully, but to tell an adult
immediately. Also, even if people are writing mean things, don’t put the email in the trash.
Instead, show it to adult as proof. Cyberbullying is serious and the written evidence can be used to stop the bullies.”

“However, the Internet is a great communication tool when we use it properly.”

**Ask students:**

“How many of you use the Internet for writing email?”

**Discuss:**

*Student responses. Most students will have email accounts.*

**Say:**

“No matter how we communicate with each other, whether through email, handwritten letters, the phone, or just talking face to face, it’s very important to exercise responsibility in using good communication manners. When we communicate, we should be polite. We should be polite when we write and polite when we talk.”

“Internet politeness or etiquette is called “netiquette”. Netiquette includes things like some simple rules for writing email. For example, don’t write email in all capital letters – it’s like shouting at your readers! Never say anything in an email you wouldn’t say in person and always avoid rude language. Be clear and concise and check your spelling. These are good communication ideas even without using the computer.”

“So let’s summarize what we’ve discussed today:”

**Discuss:**

- *Abide by rules in the Acceptable Use Agreement*
- *Don’t share passwords.*
- *Report cyberbullying immediately to an adult.*
- *Abide by the rules of good netiquette*

*If time allows, ask if students have any questions.

**Resources and Activities:**

*Grades 9-12: Managing Passwords*
http://cybersmartcurriculum.org/safetysecurity/lessons/9-12/managing_passwords/

CyberSmart!™ Student activity for grades 9-12 with downloadable PDF student worksheet to assist students developing strong passwords.

*Grades 9-12: Acceptable Social Networking?*
http://cybersmartcurriculum.org/cyberbullying/lessons/9-12/acceptable_social_networking/

CyberSmart!™ Student activity for grades 9-12 with downloadable PDF student worksheet to help students understand the dangers of cyberbullying.
Cyber Smart Week
Day 5: Check For Understanding

These questions are designed to review the Internet safety rules covered during the previous days. Questions may serve as the basis for a written quiz, a class discussion, “thumbs up, thumbs down”, or presented in any other manner that will help determine student understanding of the concepts presented. The feedback you receive from students will help you to answer the Cyber Smart Week Survey questions.

True or False

1. If you’re playing a game on the computer and a message pops up asking you for personal information so you can enter a contest, you should use your own judgment and do it.

2. It’s okay to give your name to people you don’t know online, as long as they tell you their name.

3. If a person sends you something on the Internet that is confusing, hurtful, or makes you uncomfortable, you should tell a trusted adult right away.

4. It is okay to copy sentences from a book and use them in a report as long as you put quotation marks around them and say which book they came from.

5. Copyright means that you have the right to copy DVD’s, CD’s and computer games as many times as you want.

6. If you copy facts from the Internet and put them into a report, it’s okay as long as you don’t tell anyone where you found the information.

7. It’s always appropriate to cite the information source if it is information you didn’t know before.

8. It’s okay to give your computer passwords to someone as long as they are a friend.

9. The school computer lab is a good place to download programs from the Internet and install them on the computers.

10. Writing email is similar to writing a letter and should be carefully checked for correct spelling and grammar.

Answers:

1. F – Don’t fill out online forms or surveys or enter contests without parent permission.
2. F – Don’t share personal information online such as name, address, phone number, age, gender, photo or Social Security number.
3. T
4. T
5. F – Respect intellectual property and copyright law; only download with artist permission or from copyright-free Internet sites.
6. F – Always cite your sources; never plagiarize.
7. T
8. F – Don’t share passwords.
9. F – Abide by the rules in the Acceptable Use Agreement
10. T
CYBER SMART GLOSSARY

Blog (short for web log) - A web log is usually defined as a personal or noncommercial website that uses a dated log format, usually with the most recent at the top of the page. Blogs often contain links to other websites along with commentary about those sites. A web log is updated frequently and sometimes groups links by specific subjects, such as politics, news, pop culture, or computers.

Chat - Real-time communication over the Internet. Individuals type and send messages that appear almost instantly on the computer monitors of the other people who are participating in the chat.

Chatroom - A webpage that contains a large window into which text can be typed, enabling a real-time conversation between many people at the same time. Many people can chat together simultaneously. A chat site will display the names of those who are online at any given time.

Cyberbullying - sending or posting harmful or cruel text or images using the Internet or other digital communication devices.

Cyberspace - Refers to all the computer networks on the Internet. The term distinguishes the physical world from the virtual or computer-based world.

Download – Describes the process of transferring data from one computer, often a server or large computer, to another computer.

Email (electronic mail) - A service that allows people to send messages with pictures and sounds from their computer to another computer. To send someone an email message, an individual needs an email account and the receiver’s email address.

File Sharing - A method of allowing one computer or server to send the same digital file of a document, song, image, or other media to many different end users. Shared digital files can be read, reviewed, and updated by more than one individual.

Instant Messaging (IM) - A service that allows people to send and receive messages almost instantly. Sending an instant message requires downloading and using a free software program and the IM address of another person using the same software program.

Internet - A network of millions of computers from all over the world. The Internet allows computers to trade information using telephone lines, fiber-optic cables, and satellite links. It is also referred to as the "Net".

Netiquette - Courtesy, honesty, and polite behavior practiced in Internet communication.

Online - Another way to describe having access to the Internet or actively using the Internet.

Password - The secret word used when signing onto the Internet or an online service that helps to confirm an individual’s identity.

Pharming - An online scam that attacks the Internet browser's address bar. Users type in what they think is a valid website address and are unknowingly redirected to an illegitimate site that steals their personal information.

Phishing - An online scam that uses email to “fish” for users' private information by imitating legitimate companies. People are lured into sharing user names, passwords, account information or credit card numbers. The phishing email usually contains a link to an illegitimate site. Scammers copy the look of a website to set up a nearly identical page, one that appears to be part of that company's site.

Piracy - Illegally copying copyrighted software, music, movies or other media.

Private Chatroom – Some chat websites allow people to open their own chatrooms to have one-on-one conversations with others as they wish.

Privacy Policy - The policy that a company or organization operating a web site uses for handling the personal information collected about visitors to the site. Privacy policies can often be found on websites at the bottom of the “home page”.

Message Board (or 'forum') – An Internet site where messages are left by individuals and appear as lists or ‘threads’ for others to see.

Social Networking Site - A website specifically focused on the building and verifying of social networks for whatever purpose. Many social networking services are also blog hosting services. There are currently over 850 social networking sites on the Internet including many for teachers such as “Classroom 2.0”, found at http://www.classroom20.com.

Spam - Unwanted emails, often coming from advertisers or others alerted to an individual’s email address through online purchases or other Internet activities.

Surf - To search for information on the Internet in a random, non-linear way.

Virus - A computer program that can destroy files or make a computer "crash." Viruses can be sent via email or through other file-sharing programs. Using an anti-virus software program and not downloading information indiscriminately can protect computers from viruses.

Webpage - Is a single page of data within a web site - the basic building blocks of websites, analogous to pages in a book, magazine or other form of literature

Website - A collection of "pages" or files linked together and available on the Internet.

World Wide Web - A way of accessing information over the medium of the Internet. The Web uses the HTTP protocol, only one of the languages used on the Internet, to transmit data.