Internet Safety/CIPA Lesson Plan

Social Networking

Overview

Students need to safely use the Internet for learning, socializing, and for preparing for college and work. While firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential, alone they are not sufficient to ensure your safety and security.

The more teens are online, the more likely they will be involved in some kind of harassing situation. Ultimately, Internet safety depends on the decisions you make every time you go online. As part of the Child Internet Protection Act (CIPA) schools are required to provide you with guidelines for appropriate online behavior and cyber bulling awareness.

What is Social Networking?

Social Networking is a term used to describe the fairly recent breed of websites, also referred to as online communities. These sites enable their subscribers to post a journal and various forms of media content, to generate and maintain relationships with other participants, and to engage in discussions around common interests with others.

Deciding how to present yourself online should be considered carefully. You may not always know who your audience is. Social networking sites may feel private but in reality, they are public spaces where privacy settings may or may not give you the privacy you expected.

The content you post on profiles and blogs sticks around the Internet forever, even after you decide to take it down. The information, photos, and videos you post about yourself can easily be found by searching, even if you thought you marked it private. The content you create can be copied by anyone and used for any purpose without your permission. Before you post something online, consider the "invisible" audience and remember that there is no guarantee of privacy online. Even if you use privacy controls offered by social networking sites, there will always be audiences you didn't intend to see your stuff.

It's not enough to think about how you present yourself, you also need to consider the information your friends are sharing about you. Always monitor what others are posting about you in comments, photos, videos and blogs.

There are several ways in which information on the Internet is preserved after it is deleted by the creator. Many social networking site companies keep a copy of a profile to make it easy for you to rejoin the network in the future. Search engines archive, or keep copies of, old web pages as well as current ones.

Social Networking Safety

Children, teens and adults are all targets for identity theft. Identity thieves can collect, steal and use your private identity information such as social security numbers to pretend to be you and then obtain a driver's license or get credit cards in your name.

There are many precautions you should take while surfing the Internet. **First, ALWAYS remember you should NEVER give ANY private identity information out about yourself.** While not all sites or individuals that collect information from children are illegal, it is better to be safe than sorry.

Private identity information includes your full (first and last) name, postal or physical address, e-mail address, school address, phone numbers, passwords, credit and debit card numbers, social security numbers, mother's maiden name, your parent's place of work, and photos in which you can be recognized.

It's okay to share information online about yourself that cannot be used to identify you. This is called personal information. **Personal Information** includes your age, whether you are male or female, how many brothers and sisters you have, your favorite band, your favorite food, how many pets you have, the name of your pet, and your opinion about an important issue.

Other security cautions you should take include:

- Use anti-virus software
- > Do not open email from unknown sources
- ➤ Use hard-to-guess passwords and keep them private. The most secure passwords are made up of combinations of eight or more letters, numbers, and symbols. Never use private information or information that can be easily guessed.
- Protect you computer with firewalls
- Do not share access to your computer with strangers
- Disconnect from the Internet when not in use
- Regularly download security protection updates
- Remember that on the Internet, people can pretend to be who they are not, and they may go to great lengths to sound convincing.
- Remember, Internet friendships, relationships, and conversations can never be as true, personal, and rewarding as they are in person. If you really need to talk to someone, find a friend, family member, or adult you trust.

Cyberbullying

Cyberbullying can be defined as the use of *Information and Communications Technology, particularly mobile phones and the internet, deliberately to upset someone else*. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. It differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

Cyberbullying takes different forms: threats and intimidation; harassment or "cyber-stalking" (e.g. repeatedly sending unwanted texts or instant messages); vilification / defamation; exclusion or peer rejection; impersonation; unauthorized publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images); and manipulation. Cyberbullying is clearly deliberate and aggressive.

Bystanders can also easily become perpetrators by passing on or showing to others images designed to humiliate, or by taking part in online polls or discussion groups. Students may not recognize themselves as participating in bullying, but their involvement compounds the misery for the person targeted. Students need to be aware that their actions have severe and distressing consequences and that participating in such activity will not be tolerated.

Cyberbullying, like all bullying, is taken very seriously and is **never acceptable**. There are criminal laws that can apply in terms of harassment and threatening and menacing communications. If it is taking place on school grounds, such as through the school's computer network or on students' cell phones, the school may be justified in taking action.

Responding to Cyberbullying

If you are being bullied, you should keep copies of texts or emails received to aid in any investigation. There are also additional reporting routes available, through mobile phone companies, internet service providers and social networking sites.

Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. If you find yourself in this kind of a situation, talk to your parents, teacher or another adult immediately to let them know what is going on. Whether the incidents are happening at school or work, the police should be contacted as soon as you receive threatening or harassing emails or discover inappropriate postings. If the incidents are happening at school, inform your teacher so the school can check their computer system and computer logs to identify suspects and aide the police in their investigation. The police can contact the service provider and work with them to have the content or links removed. Do not retaliate or reply to the individual. Try to block or remove people you suspect from your buddy list. Think carefully about what private information you may have in the public domain.

Cyberbullying can cause an individual to feel isolated from family and friends. The feeling of humiliation can be so strong that it can cause the person to take desperate action and do something they would not normally do. **THINK** before you post anything about someone on a social network. Ask yourself these questions:

- ➤ How will this make someone feel?
- > Do I want to be responsible for any harm my actions cause?
- Would I want the same thing or something similar posted about me?
- Could this lead to criminal charges or cause me to lose Internet privileges?

It is important to remember that information you send as a joke, may not be received as one.

Preventing Cyberbullying

Cyberbulling is strictly prohibited at school. At school means in a classroom, elsewhere on school premises, on a school bus or other school-related vehicle, or at a school-sponsored activity or event whether or not it is held on school premises. At school includes conduct using a telecommunications access device or telecommunications service provider that occurs off school premises if the telecommunications device or service provider is owned by or under the control of the school district.

The best way to prevent cyberbullying is to raise awareness of this issue with students and parents and ensure that any incidents are stopped before they become too serious or upsetting. Understanding the damaging effects cyberbullying has on an individual is crucial. Education and discussion around the responsible use of technologies and e-safety are key to preventing cyberbullying and helping you deal confidently with any problems that might arise, whether in or out of school.

Internet Chat Rooms

Chat rooms are places online where groups of people can carry on a conversation. They are the hardest of the communication tools to manage. Because of the truly anonymous nature of chat rooms, anyone including individuals who don't have good intentions lurk in chat rooms pretending to be just another interested party. Chat rooms are probably the most dangerous part of the Internet because of the ease of contact and because they're often organized around subjects like sex or cults or dangerous physical acts that attract dangerous people.

There are different levels of supervision in chat rooms. Some are open environments with no moderation; some have leaders who moderate the discussion; while others have monitors who assess what people write before anyone else gets to see it. If you misbehave, these live monitors can reprimand you or even kick you out. These are the safest types of chat rooms you should use.

More than any other place online; chat rooms are cruising grounds for pedophiles and other predators trying to make contact with young people. In the anonymous atmosphere of the Internet, where kids feel free to be honest, conversations can quickly become intimate. Some chat rooms offer users the option of going into private rooms, or sharing private messages (PMs) that no one else can see or monitor. **Never let yourself be lured out of the public area and into a private chat room**.

Chat Room Do's and Don'ts

- **Don't include any part of your name**, date of birth, location, or anything sexually suggestive in your 'chat' name.
- > Don't go in to private chat rooms.
- When choosing an online chat room, **be cautious of the chat room name**. Stick to chat rooms created by the online service, rather than 'member created' rooms.
- > Don't say anything in a chat room that you wouldn't say in public, in front of your parents or friends.
- If you start to chat regularly with someone, keep your parents informed.
- Remember, you are in control. If a conversation starts to get strange or make you feel uncomfortable, then leave. Leave the chat room, and log off.
- Never meet anyone face to face that you met on the Internet unless you tell a parent or adult first, and they go with you.
- > Don't think of people you've met on the Internet as 'real life' friends. They're just not!
- > **Don't click on links or go to sites** that you're not familiar with.
- Never post a picture of yourself online and never e-mail pictures of yourself to people you don't know.
- Never give out your password and make sure it's something only you know.
- > Don't respond to 'flames'- people trying to start an argument, or insults, bad language, etc.
- > Be suspicious of anyone who tries to turn you against your parents, teachers, or friends. They may have a hidden agenda.
- Use a different chat name (if possible) than your user name or e-mail address.
- **>** Be wary of **ANYONE** who wants to know personal information about you.

Classroom Activities:

- 1. Have students write and take a survey of other students in your school to find out about their cyberbullying experiences. Have them collect the data anonymously and report their results to school administrators by age and gender.
- 2. Have students write and publish a "quick guide" about cyberbullying, including what to do when it happens and where to go for help.
- 3. Have students collaborate to create a tip sheet for students affected by cyberbullying, and publish it on a school web page or a flier.

- 4. Have students plan a school-wide cyberbullying prevention activity and get others to sign on. Set a goal for the minimum number of people you want to participate. When that number of people sign on, take your planned action.
- 5. Hold a poster contest invite students to design cyberbullying prevention posters. Ask some teachers, administrators, and parents to judge the entries.
- 6. Have students write and conduct a survey to find out your school staff's perceptions of cyberbullying. Have them compare these findings to a survey of students and present their results to the staff.

Resource websites for teachers, students and parents:

www.remc12.org

www.cybersmartcurriculum.org

www.teachersfirst.com

www.csriu.org

www.stopcyberbullying.org

www.cyberbullyhelp.com

www.staysafeonline.org

STUDENT PARTICIPATION ACKNOWLEDGEMENT FORM

| I have participated in the Social Networking, Cyberbullying, and Chat Room classroom informational session at my school. I understand the safety rules and ethics for social networking sites and chat rooms. I understand the definition of Cyberbullying and the impact it can have on people. I am aware that the school has no tolerance for inappropriate online behavior or Cyberbullying and that it could lead to loss of my Internet privileges and/or criminal charges. | |
|---|---|
| Student Signature | Date |
| I have reviewed and discussed the Social Networking, Cyber with my son/daughter. I understand the safety rules and et understand the definition of Cyberbullying and the impact t school has no tolerance for inappropriate online behavior o son/daughter participates in unacceptable Internet behavior my son/daughter's Internet privileges and/or criminal charge | chics for social networking sites and chat rooms. I hat it can have on people. I am aware that the r Cyberbullying. I understand that if my or and/or Cyberbullying that it could lead to loss of |
| Parent/Guardian Signature | Date |