

Internet Smarts

Keeping Personal Information Private

Teachers Guide

Although the student lesson focuses upon the dangers of meeting people online and giving out personal information online, there are other additional areas that teachers should cover that deal with Internet safety. At the end of this guide there are discussion questions specific to the lesson, but in this section you'll find information on other dangers kids face as well.

Background Material

Introduction:

Don't let the media scare you into thinking that the Internet should be off-limits to your students, even if they are in elementary school. Sure, you've read horror stories, and you know that the more your students use the Internet, the more likely they are to encounter problems. You'll need to set up rules just like you do for everything else that goes on in your classroom, but that's no reason to keep your students from learning to use the powerful communication and learning tool the Internet has become. There's no getting around Internet use today. You've got to prepare your students for using it correctly.

Some of the dangers kids face online won't be as much of a problem at school as at home. Generally, students' work on computers at school, especially at the elementary levels, is monitored. That's not to say that some of the things kids do won't get by your eagle eye, but for the most part, you'll know what your students are doing online. Therefore, although you'll definitely want to continue monitoring, you'll also want to teach your students how to use the computer safely at school as well as at home.

Finding Information on the Web

Visualize the Internet as a giant library packed with treasures and junk. There're no librarians to help your students with selections, there're no editors to decide what is published, and there're no signs leading the way to the good stuff or the safe stuff. If your students know how to be safe online and where to go to get the information they need, there's no quicker and more current source of information anywhere.

The best way to make sure your students avoid problems when searching for information, including happening upon inappropriate sites, is to give them the exact sites where you want them to get specific information. In addition, you'll want to make sure they have access to a list of more general "Starter Sites" - places where they can begin looking Sites" to your Favorites or Bookmarks in your computers at school. (See a list of suggested sites in the Additional Resources.) Depending upon their age level, lead them to sites like Yahoo!Kids (<http://kids.yahoo.com>), Ask Kids (<http://www.askkids.com/>), SortFix (<http://www.sortfix.com>), and Ask (<http://www.ask.com/>).

Sometimes it may be necessary to type in Web site addresses (URLs) into the address area of a browser. If copying and pasting isn't possible, stress that they should take care typing in an URL. Some adults-only sites have addresses very similar to those sites your students may want to visit for their assignments. Probably the best-known example is the White House site, whose real address is <http://www.whitehouse.gov/>. If students type .org instead of .gov, they'll find themselves on a site that spoofs the President and adding .com takes the kids to an adults-only site.

Your students need to know that all places on the Internet are not appropriate for them, and they should be aware that if they happen to land in a site that has content that is upsetting to them that they should keep the site open and let you know right away.

Some students may go to an inappropriate site on purpose, usually to impress peers. Your rules for dealing this should be set. Make the penalties for misuse of Internet access clear. Okay, you ask, how do I know if a student came upon a porno site by accident or not? That's not always easy to know, but you can probably tell by asking how the student got into the site. For example, if they were to go to the White House site and typed .com instead of .gov, most likely it's a mistake — unless they have heard of the adult White House site and want to open it to get a laugh. It's always better to take the child's word for what happened, at least the first time. After all, haven't you happened into an adults-only site and had trouble getting it off your screen? Most of us have, even if we haven't gone there on purpose.

Some teachers think they don't have to supervise their students carefully because their school has invested in a firewall and filtering or monitoring software. Actually, what the firewall does is to try to keep people out of your school site, especially hackers. Filtering software attempts to let students in your school visit only acceptable sites. The best filters, however, are not software or hardware, but you and your students' parents. Although filters (software that keeps your students from questionable sites) and monitors (software that keeps track of where your children are going online) are helpful, you can't rely on them entirely. You've got to be attentive to what your students are doing. Just like you can't be completely trust a substitute teacher to supervise as you would, you can't put all your trust into an Internet filter or monitor.

Dealing with Email, Texting, and Social Networking

Before (or if) your students get school email accounts, they'll need to know about responsible uses of email. You should set up rules for types of email they can send, when they can use email, and your expectations as to content. Let them know that their email is not private and that they will be responsible for what they write. Make it clear that they shouldn't open email from those they don't know and that attachments from unknown sources or from someone they met online should never be opened. Remind them that those attachments may contain viruses that could attack the school computers.

The fact that people on the Internet can be anonymous presents dangers to your students. Kids, even teens, tend to be trusting when they "meet" people online through social networking, games, etc.. If someone claims to be a 14-year-old boy, it probably wouldn't cross a student's mind that that person could be a 35-year-old man or woman or even a female classmate. Your job as a

teacher is to help your students learn how to handle themselves online so that they will not be vulnerable to those who are not who they say they are. Keep in mind, in addition, that your students may use their own online anonymity to experiment with language you would not approve of while texting, emailing, social networking and using other forms of digital communication.

Remind your students that the cardinal rule when they are online – whether social networking, texting, gaming, emailing - is to not give their real name, school, address, telephone number, picture, or any other information that could identify them. “Oversharing” is the number one issue in trying to keep personal information private and these days hackers and predators have trained themselves to pick up the bread crumb trail of personal information that students unwittingly leave behind. Students should be cautioned, in addition, never agree to meet anyone they've met online without their parents' permission, and if their parents give their permission, their parents should accompany them to meet the person.

Lesson Overview

The student interactive slide show is an unfinished story about a fifth grade girl who gets involved online with someone she considers a cool, new friend. In the lesson, students consider various endings to the story as they tackle the problem of exactly who this "friend" might be and what might happen in different scenarios.

The lesson is not meant to scare your students, but instead to help them toward understanding what it is safe to do online. The idea is to get them to realize although the Web is wonderful, they have to be careful there just like they do in their community. They certainly wouldn't walk up to a total stranger on the street and give that person their telephone number or their picture.

Bottom Line and Over Time

- Discuss use of the Internet (both through computers and digital devices like cell phones) with your students, and keep channels of communication open so that they'll talk with you about what they are doing online. Remember that the foremost reason students give for not discussing the problems they encounter online is that they are afraid teachers and parents will take their digital privileges away.
- Make class rules for use of the Internet clear and make it clear that they will be added to as the need arises.
- Let them know that there will be consequences if they do not follow the rules.
- Supervise them even if you have filtering or monitoring software installed.
- Keep in mind that no matter how bright your students are, that they can be exceptionally naïve when it comes to people they meet online.
- Talk with them about safe ways to use the Internet at home.
- Remind them to be careful not to “overshare” information. Sometimes even seemingly harmless personal details can give their identity away.

Discussion Guide for the Lesson:

1. Before starting the lesson, students should take the online poll to see how their ideas compare with other students in the NYC Metro region.
2. Ask the students to read the open-ended story presented in the lesson either individually or have it read-aloud by class members.
3. In the “Review the Scenarios” section go over each scenario with the students. Let them role-play the scenes acting out as many different endings as they can imagine. They need to decide what happens next. The scenarios are:

Scenario One

Gwen's parents go to the mall to see who Tiffany and Jake are. Would they find that Tiffany is really a sixth grader who is a cheerleader, or could Tiffany be someone else? Maybe Tiffany is 20-year-old woman. Maybe Tiffany is a 13-year-old boy or a 55-year old man pretending to be a sixth grade girl.

Scenario Two

Gwen sneaks out of the house and takes the bus to the mall. She meets Tiffany and Jake, and they all go to the movies. When she comes out of the theater, her father is waiting for her.

Scenario Three

Gwen and her mother go to the mall to meet Tiffany. They wait outside the pizza shop, but no girl in a pink sweater is there. In school on Monday, the kids are all laughing as Gwen comes into the room.

Scenario Four

Gwen sneaks out of the house and takes the bus to the mall. She doesn't see a girl in a pink sweater, but instead a guy, who looks about 17, asks her if she is Gwen and introduces himself as Jake. He asks her to come with him to see Tiffany.

Scenario Five

Gwen dries her tears and tells her mother that even though she will be embarrassed she is willing to have her mother go with her to meet Tiffany. Her mother gives her a hug and tells her to text Tiffany that she will meet her. Gwen tells Tiffany that she has to bring her mother along.

4. Talk with the students about the following questions, which appear after the scenarios.

Why do you think Gwen's mother is so worried?

She's worried because she wants her daughter to be safe, and she knows that if isn't safe for kids to agree to meet people they've met online unless they have their parents' permission and unless their parents go with them to meet the person.

Why would someone pretend to be someone they aren't?

Some people are just trying to be funny or to embarrass other people. They might think it's neat to act like somebody else. Teenagers might do it to make fun of younger kids like Gwen. The real risk, though, is if someone dangerous arranges a meeting with a kid and the kid goes because he or she thinks the person is another kid.

Suppose a kid finds an adult online who will listen to him or her. The person is very nice and easy to talk with. Is this person okay to meet?

No, absolutely not! The same rules apply. Kids should tell their parents if they are "talking" with any adults online, and they should never plan to meet them face-to-face without their parents permission and unless their parents are with them.

What things did Gwen do wrong that might put her in danger?

First of all, she thought she really knew someone she didn't know. Second, she gave a person she met online personal information about herself. Third, she didn't follow her parents' rule about not texting people she didn't know. Fourth, she went online late at night. Fifth, she lied to her mother.

5. It's always easier to follow the rules when you've had some say in what they are. As a conclusion to the lesson, have the students make a class list of rules for home and school Internet safety to post in the classroom or computer lab. Students can enter the rules into the rulemaker and print out a copy for their homes and for the class or computer lab. The major rules that should be included on that list are:

- Do not give out any personal information online to someone you really don't know. This information includes your name, telephone number, photograph, address, school, or anything that can identify you. For example, if you say you like to go to a certain park or store, if you say you're going to be in a dance recital at the community center, that's giving personal information.
- Do not text, social network, or email with people you don't know. You don't know people you've met online.
- Don't join a social network unless in you are not old enough for the age requirement. Be very careful who you friend on social networks and what information and photos you post.
- Be careful of what information you send out through your cell phone.
- Only open email and texts from people you know and organizations you trust.
- Do not open any email attachments that come from people or organizations you do not know.
- Show respect for others online.

6. Address with students whether the lesson changed any of their ideas about Internet safety.

Additional Resources

Teachers: Please note that some of these resources are targeted to families, but they should be useful to you as well.

Wired Safety

<http://www.wiredsafety.org/resources/biographies/parry/index.html>

BBC Safety Online Resources

<http://www.bbc.co.uk/onlinesafety/>

Google Safety

<http://www.google.com/familysafety/>

Social Networking : Safety Tips for Tweens and Teens

<http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm>

School Safety and Security

<http://www2.scholastic.com/browse/article.jsp?id=4395-top>

Family Internet Health & Safety

<http://familyinternet.about.com/library/safety/blsafety1.htm>

Child Safety on the Information Highway

<http://www.safekids.com/child-safety-on-the-information-highway/>

GetNetWise

<http://kids.getnetwise.org/tools/index.php>

Family Internet's Safety & Privacy Online

http://familyinternet.about.com/od/computingsafetyprivacy/Computing_Safety_and_Privacy_Online_and_in_the_Home.htm

BBC Online Safety

<http://www.bbc.co.uk/chatguide/>

Surfnet Kids List of Monitored Chats

<http://www.surfnetkids.com/chat.htm>

Great "Starter Sites"

National Geographic

<http://www.nationalgeographic.com/>

Smithsonian

<http://www.si.edu/>

NASA

<http://www.nasa.gov/>

Biography

<http://www.biography.com/>

The American Library Association's Great Web Sites,

<http://www.ala.org/parentspage/greatsites/amazing.html>

The 50 States

<http://www.50states.com/>

Altapedia Online

<http://www.altapedia.com/>

How Stuff Works

<http://www.howstuffworks.com/>

The History Channel

<http://www.historychannel.com>