* CLASS AND INTERNET RULES AND SAFETY *

This expedition and the next have a lot in common. In this lesson, you will further explore the class rules and guidelines for Internet safety. In the next lesson, you will look at the legal and ethical rules that guide the Internet. Much of this is common sense. Some guidelines may surprise you. You may have accidentally violated a few safety rules without knowing it. This expedition will help you understand both the rules and why they're important.

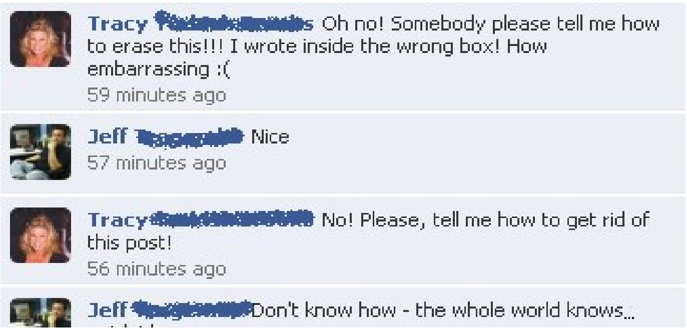
This expedition is divided into sections. Each section discusses particular rules and dangers on the Internet. You will need to know all of the principles contained in this and the class rules in order to complete this expedition.

GENERAL INTERNET RULES...

Privacy...

Nothing on the Internet is private. Your websites are tracked. You need to be aware of these facts when you are on the Internet. Some sites tracking you may include your search engine (such as Google), your social media sites (such as Facebook), your email (such as Gmail), and your individual computer. Remember that nothing online is private.

Permanence...



Tracy [redacted] Oh no! Somebody please tell me how to erase this!!! I wrote inside the wrong box! How embarrassing :(
59 minutes ago

Jeff [redacted] Nice
57 minutes ago

Tracy [redacted] No! Please, tell me how to get rid of this post!
56 minutes ago

Jeff [redacted] Don't know how - the whole world knows...

Actual Facebook comments after embarrassing post

Once something is on the Internet, it is permanent. All posted information can be accessed at a later time, even if you believe you have deleted it. There are programs that save older versions of websites, and Internet hosts can keep data posted on their sites. Once you release the information to the web, you lose all control over it.

Even if you aren't concerned about stored files, you should remember that if you email, text, or post something, not only do your friends have a copy, but it may continue onward to their friends and acquaintances. It doesn't take many steps before you've lost control of your pictures or information.

POSTING INFO ABOUT YOURSELF...

Private Information...

As much as possible, your personal information should remain private. It should never be posted where strangers can access it. Private information should include your last name, pictures of you, your home address, your school, your phone number, and your email. These items should be guarded so that they are not accessible to strangers.

Another item to keep private is your screen name. You shouldn't include personal information in this name. This includes your birthday, or any identifiable data. It's even risky to include data that identifies your gender. So tuffguy99 may be a security risk.

Use of Your Information…

Your online information will be used by several sources. Companies pay for your information so they can sell you items. If you are receiving any services for free, your information is being sold.

Many people can access your information. Employers often look at an employee's Facebook or other social media accounts to determine who to hire. They look at posts to determine whether the person is responsible, and at pictures posted. They don't want employees who would embarrass the company.

Real Facebook pic, caption added

If you are ever in a legal battle, lawyers often will look at your online information for ideas on how to win their case. Many people are in jail because of things they posted.

Again, whatever you post online is permanent. As quoted in the *Wall Street Journal,* the Google CEO (the boss) Eric Schmidt said,

> "'I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time,' he says. He predicts, apparently seriously, that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites." (Article by H.W. Jenkins Jr., August 14, 2010.)

That picture of you trying to look cool for the camera, you and your friends being silly, that embarrassing picture your cousin took... all of them are online. Please think before you post, both information about yourself and others.

PASSWORDS…

Passwords are meant to be absolutely private. They are intended for you alone. Because you are a minor, and your parents are responsible for you, you should share your passwords with your parents, but no one else. Not even your best friend should know your passwords. The more people who know your password, the greater the risk of problems.

Sharing a password is not a way of showing trust or being closer friends. It can leave you with huge risks. Even if your friend never violates your trust, if you were "hacked" (or your account was accessed by an outsider), you would have doubts and concerns about your friend. Please keep your passwords to yourself.

DOWNLOADING DANGERS…

Whenever you download a program, you give it access to your computer. Most well known and respected programs do not abuse the data, but suppose you find a game online with a free download, or a music sharing site that lets you have anything if you will only download their program. Sites such as these frequently have evil programs attached. These may be spyware (that will spy on your computer, finding private information), or other types of malware (and mal means bad – these are destructive programs). Spyware is the biggest threat to computer safety today. It records your personal information, can steal passwords, flood you with pop-up ads, plant viruses in your computer, turn your computer into a secret server for pornography, can redirect your browser to sites you don't want to go to, and will slow down or crash your computer.

Whenever you want to download a program, first check with the owner of the computer. In class, the teacher has some say on what is downloaded. At home, the owners of the computer (probably parents) should be consulted.

If you have permission, first consider whether the download is absolutely necessary. If it is, decide whether you are downloading from a trusted site. A search online should help you learn whether there are known problems. If you continue and begin a download, remember that if you have to enter too much personal information, something is wrong. Do not continue the download. Also, if the program wants to install a lot of other programs (such as toolbars), you may want to think again.

SOCIAL NETWORKING APPS...

Speaking of downloads, there is a unique problem with social networking and downloadable apps. If you were on Facebook, and you saw a quiz entitled “How well do you know fairy tales?” you could click on it and take the quiz. If you pay attention to the little pop-up notice, you will learn that by taking the quiz, you're giving the creator of the application permission to use your personal data. They have the right to view your information. The same may be true of many cell-phone apps.

Not only do those companies have permission to view your data that one time, but as long as they'd like. Be careful about online quizzes, personality tests, and how many places you “like.” If you “like” Walmart, you will notice a lot more of their ads on your page. Your information is being used.

PORNOGRAPHY...

Pornography includes nude (naked), or partly nude pictures of people. It is nearly everywhere online. Sometimes you may have a perfectly innocent search, or click on a link, and pornography may appear. If you do spend time on inappropriate sites, it can cause extreme challenges as it becomes part of your life. There are many reasons why porn is such a big problem.

What should you know...

Pornography is a huge business. People that manufacture porn make money by exploiting people. They ruin lives and don't care. Pornography is fiction. It does not teach anything about real relationships, love or commitment. It isn't truth. Pornography is also extremely addictive. What may start off as curiosity, or even a joke, could end up changing the brain of the viewer. Manufacturers know this, and will sometimes place pornography on sites where innocent people could stumble across it. Some people get so addicted that lives and marriages have been ruined. Pornography is dangerous.

What should you do at school?

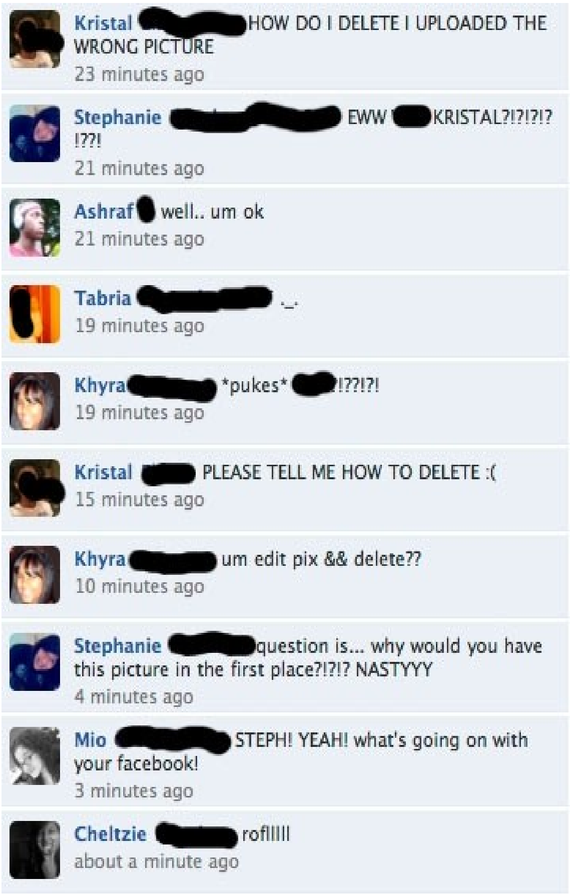
Sometimes when browsing innocently, you may stumble across a site with pornography. If this happens at school, immediately shut the computer OFF! If there is an infection in the computer, this will prevent it from spreading. After the computer is off, immediately inform the teacher. Most likely, this will be the end of the incident. Reporting the incident as soon as possible will reduce the chances of future problems. If possible, remember what links you were following when you found the inappropriate pictures.

What should you do at home?

If the same thing happens at home, you should do the same thing. Make sure you tell an adult. Secrecy is the biggest problem when it comes to pornography. If you find that you already have a problem, you need to tell a parent. Make sure you're only using computers in places where you can be seen, and avoid private rooms. You may want to talk to your parents about having a filter installed on your computer.

Self-made pornography – rules...

Taking pictures of yourself that are inappropriate is considered pornography. It is highly illegal to make such pictures of underage people, including yourself. If you send them to friends, you have just distributed child porn. This is punishable by law. Never send any pictures that could violate the law. And always remember that once you send it, you can't get it back.



Kristal [redacted] HOW DO I DELETE I UPLOADED THE WRONG PICTURE
23 minutes ago

Stephanie [redacted] EWW [redacted] KRISTAL?!?!?!? !??!
21 minutes ago

Ashraf [redacted] well.. um ok
21 minutes ago

Tabria [redacted] ._.
19 minutes ago

Khyra [redacted] *pukes* [redacted] !??!?!
19 minutes ago

Kristal [redacted] PLEASE TELL ME HOW TO DELETE :(
15 minutes ago

Khyra [redacted] um edit pix && delete??
10 minutes ago

Stephanie [redacted] question is... why would you have this picture in the first place?!?!? NASTYYY
4 minutes ago

Mio [redacted] STEPH! YEAH! what's going on with your facebook!
3 minutes ago

Cheltzie [redacted] roflllll
about a minute ago

Real comments after embarrassing picture

OTHER DAMAGING SITES...

If you come to a site that starts giving you a lot of pop-up ads, or if something starts downloading without your permission, turn your computer off. It is probably a malicious (meaning bad) site. Follow the same procedure you would with porn sites.

Bad sites may also include hate sites, violent sites, sites meant to intimidate or harm, or anything that can cause classmates to feel uncomfortable. Please do not go to any harmful site.

STRANGER DANGER...

People that you meet online are strangers. Some people have fantasy lives online where they pretend they are someone else. Fifty-year-old men may pretend to be twelve-year-old girls. Prison inmates may pretend to be a boy from a neighboring town. There is no way to tell. Never, ever give personal info to someone online. And if you want to meet in person, always go with a trusted adult. Never send a picture to a stranger.

BULLYING…

Bullying is any time that a person uses force, intimidation, humor, gossip, or other unkindness to make someone else feel bad. Bullying is very common, but it is wrong. Bullying can happen on the computer. It may include unkind posts on social media, hacking a person's account, threatening or mean emails, unwanted texts, the use of pictures to humiliate, or online gossip.

If you are being bullied, never respond. Most bullies want to know they got to you, and that they hurt you. Do not delete the evidence. If the bullying continues, you will want proof to show the authorities. Then tell a trusted teacher or parent about the event. The person may face trouble from their parents, school authorities, or even the police if the harassment continues.

If you have been a part of bullying, stop. It is unkind, and possibly illegal. Sending threats or intimidation can get you in trouble with police. And nobody likes a bully.

ADDICTION…

Warning: Computers are addictive. People are becoming more and more dependent on computers. One young girl responded, “I love the computer. It's where my friends live.” As technology becomes a bigger part of life, real face-to-face relationships are harmed. Too many computer hours detract from other important things people should be doing.

Social media is addictive. Sites like Facebook and Twitter rely on constant status updates and friends or followers. Limit your time on these sites. Some social media include games. Be aware that if there is no “win” on a game, it is meant to addict. It is dangerous to have various levels without an end to the game. People will not stop playing. Often these games have time limits, or require the user to be online daily (or hourly) to maximize points. This is created addiction.

Speaking of games, many computer games today are highly addictive. You can find out how addicted you are by asking a few simple questions.

1. Is most of your free time spent playing games?
2. Have you lied to friends or family about gaming?
3. Do you feel cranky or irritated when not playing the game?
4. When you aren't playing, do you often think about playing?
5. Do you get so involved you have neglected eating, sleeping, or bathing?
6. Have you skipped school or activities to play?
7. Do you sneak time to play games, such as when everyone is sleeping?
8. Do you feel most happy when playing games, or use it as an escape?
9. Is more time is spent with computers or controllers than with people?
10. Do you find yourself playing for increased amounts of time?

A yes to ANY of these may signal addiction. Get help, stop playing games, and find things in the real world to get involved with.

CONCLUSION…

Computers are wonderful tools, but there are often risks. When you know some of the traps, you can avoid them. Be safe online.