Name:
Lesson 3: Internet Life and Privacy

Digital Footprint – Privacy
- Digital Footprint: Online _____ trail
- Personal information: any information that can be used to _____ you in real life or give any access to your money or family.
- Social network: Online community of people with _____ interests, or the Web site or online service that the community of people uses to communicate.

Social Media Privacy
- Use just your first name or a _____ (false name)
- Profile pictures are _____ public – use avatars
- Set your profile to _____
- Never use your home or _____ for contact information on social media. Use e-mail addresses only.
- Check out the privacy _____ on your social media sites.

Social Media
- IP addresses are like _____ numbers for computers. Sometimes when people behave badly online, the police may use that IP to track the user down.
- Consider saving text or instant message conversations. They can be a big help in _____ someone down that is bothering or bullying you.
- There are lots of things you can post online about yourself, photos, art, videos, poetry, and personal profiles. Remember, the internet is an open environment and _____ can find these things. Information on the internet is routinely kept for many years and future schools, employers, or even boyfriends/girl-friends can find this stuff online.
- Be safe and focus on only putting _____ things online.

Top Tips
- Treat your _____ like your toothbrush – don't share it with anyone and change it often.
- Always remember to _____ when you have finished with an online service.
- Use your own digital _____ to remember your favorite websites like the history or favorites func-tions.
- Remember that most websites you visit will make a ____ of your visit and may also track the websites you visit before and after their website!
- Let an _____ know if anything you read or see makes you feel worried or upset.
- Research social media _____ settings and use them.

Identity theft
- Don't give out your _____ information to anyone you meet online that you wouldn't give it out to face to face.
- Be _____ of personal information posted online or on social media like Facebook, Instagram, Twitter, etc. Others may use this information to pretend to be you.
- Never let others use your online accounts, _____ your information.

11 Tips
1. Use privacy _____
2. Keep a list of accounts you have and delete ones you no longer use
3. Don't over share
4. Use a _____ keeper

5. Google yourself
6. _____ linking accounts
7. Use a _____ email
8. You don't need a dozen email accounts
9. "Sending" is like _____ forever
10. Searches are social:
   Web sites keep ALL information, private or not, for _____ purposes – including websites you visit
11. Manage your _____ footprint:
   - Disconnect (Disconnect.me), DoNotTrackMe (Abine.com) and Ghostery (Ghostery.com) are examples of cross-platform extensions that block tracking _____ and give users control over site scripts
   - Private browsing

Netiquette

Netiquette is the do's and _____ of online communication:
the rules of polite interaction online:
- Be _____ of everyone.
- Do not be too quick to take _____.
- Use _____ and acronyms to convey meaning.
- Protect others' privacy. Do not give out information or share posts or pictures without their _____.
- _____ your language.

Cyberbullying

Cyberbullying is any _____ behavior that takes place using electronic technology as opposed to in person
- Do not respond to or forward _____ messages.
- Keep _____ of cyberbullying.
- _____ the person who is cyberbullying you.

Acceptable Use

Acceptable Use Policy (AUP) is a set of rules you ____ follow in order to use a Web site or Internet service
- Do not _____ any state or federal laws.
- Respect others' rights.
- Do not knowingly _____ viruses or other malware.
- Do not try to gain access to _____ areas or others' accounts.
- Respect others' copyrights and _____ property.
- Know the rules and report _____.

Safety Tips

- Avoid peer-to-peer sites or _____.
- Only download from well-known and _____ sites.
- If your browser pops up a _____ message about the site you are on or the file you are downloading, exit the site immediately and run a virus scan.

Build a Secure Online Identity

Provide a detailed answer to each question below.

1. What do the privacy settings on social networking sites actually control?

2. How should you set your privacy settings? Why?

3. What personal information should you NOT post on a social networking site? Give at least three examples.

4. What should you consider before posting anything (a profile, message, comment, image, and so forth) to a social networking site? List at least three examples.

5. How can you decide whether or not to make someone your "friend" on Facebook? List at least two things you should consider.

Case Study: Attacked from All Sides
Directions
Read the following case study scenario. Then complete the assignment that follows as directed.
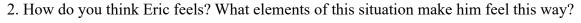
Scenario
Eric gets a lot of pressure from his parents to do well in school. Other kids in school tease him because he works so hard but still gets poor test scores. He gets instant messages and text messages during the day and at night about his poor grades. The word "loser" is in most of them, and the language becomes stronger every day. Today he received a text from a number he did not recognize, with a photo of his body with a turkey's head. A thought bubble above the picture reads: "Why am I so STUPID? What an idiot I am." Eric thinks Alexis, the most popular girl in the eighth grade, is behind the message.

Assignment
Use the following questions to create a summary of your thoughts.
1. What forms of cyberbullying did the students use on Eric? What is your evidence?

2. How do you think Eric feels? What elements of this situation make him feel this way?

3. Do you think Eric should tell his parents about the cyberbullying?

4. What qualities do you think a "trusted adult" should have? Who are these people in your life? In what ways can a trusted adult actually be effective?

5. If Alexis was the bully, what could school personnel, such as the principal, do or say to Alexis to make her realize that her behavior is wrong?

6. Have you ever been part of, or heard of, a situation similar to this? If so, share the story with the group without using names or details.

Cyberbullying 10-Tip Plan
In this activity you will create a definition for cyberbullying. The resulting definitions will then be used to create a 10-Tip Plan for display near computers.

1. Create a definition for cyberbullying.

2. Identify key words or phrases that describe the acts, the methods, the consequences and the counteractions of cyberbullying.

3. Choose key points to make one overall definition.

6. Choose key points to create 10 tips for counteracting cyberbullying.
Examples might include:
. Treat others with respect.
. Keep passwords secret.
. If you do not want the world to know, then do not post it!
. Never post personal information online that can identify you in any way.

Tip:

Tip:

Tip:

Tip:

Tip:

Tip:

Tip:

Tip:

Tip:

Tip:

Lesson 3 Quiz

1. Which of the following is an example of a strong password?   **Answer Choice**
    a. johnsmith
    b. JohnS12345
    c. JohnS@12#cookies
    d. johnsmithtoledohighschool

2. What is a cyberbully?   **Answer Choice**
    a. A computer security system
    b. A bully that intimidates people at school
    c. A bully that intimidates over the Internet
    d. A Web site that allows posting of hurtful messages

3. What should you do if you or someone you know is being cyberbullied?   **Answer Choice**
    a. Tell your parents or a trusted adult
    b. Stand up for yourself and bully back
    c. Spread gossip at school about the bully
    d. Ignore the situation and it will eventually stop

4. Which choice lists all the electronic devices that can be used to bully others?   **Answer Choice**
    a. Mobile phones, computers, tablets, and Internet-enabled gaming consoles
    b. Mobile phones with or without Internet access
    c. Desktop computers and tablet computers
    d. Internet-enabled gaming consoles

5. How do you know when a Web page you are using has a safe, secured connection?   **Answer Choice**
    a. If it is your friend's site, then it is safe.
    b. If the Web address looks legitimate, then it is safe.
    c. A red flashing pop-up message informs you that the page is safe.
    d. A lock appears in the top-right or bottom-right corner of your browser.

6. The _____is a contract that students and parents sign to make sure everyone in the school
community is safe when they use technology at school.   **Answer Choice**
    a. Password List
    b. Spoofed Site Notice
    c. Acceptable Use Policy
    d. Copyright Infringement Policy

7. Viruses, worms and Trojan horses are all examples of _____   **Answer Choice**
    a. filters.
    b. spyware.
    c. networks.
    d. malware.

8. An online community of people with a common interest who use technology to communicate with
each other and share information is known as: **Answer Choice**
    a. cyberbullying.
    b. a digital footprint.
    c. a social network.
    d. antivirus software.

9. Which of the following is an example of using netiquette?   **Answer Choice**
    a. When you scan your computer for viruses
    b. When you report cyberbullying
    c. When you are respectful online or protect the privacy of others
    d. When you are very careful about protecting your personal information

10. Which of these is a true statement?   **Answer Choice**
    a. Cyberbullying isn't as bad as real bullying because it's not in person.
    b. Cyberbullying is real bullying, just in a different way.
    c. Cyberbullying doesn't count if you only know the person from chat rooms or social media, not in real life.
    d. Cyberbullying can't get you in trouble like real bullying.

11. Which of these things is true about malware?   **Answer Choice**
    a. Malware can't harm your computer.
    b. Malware is difficult to find.
    c. A virus is different from malware.
    d. Malware can be downloaded without you even realizing it.

12. What's the purpose of a strong password?   **Answer Choice**
    a. It's harder to remember.
    b. It's easier to hack.
    c. It's harder to hack.
    d. Programmers think it's funny to make you come up with weird passwords

13. To keep yourself safe in places like chat rooms, you should: **Answer Choice**
    a. Never give out any information about yourself.
    b. Use a pseudonym.
    c. Use a profile picture that's not a real picture of you.
    d. All of the above.
    e. A and B only.
    f. A and C only.

14. Aaron and Scott decided to upload some music they'd written and recorded to YouTube. They got reviews on it. Some of those reviews were extremely mean. Which of these is not true about those reviews?   **Answer Choice**
    a. They might violate YouTube's Acceptable Use Policy.
    b. If someone only says something mean once, it is still cyberbullying.
    c. Aaron and Scott can block people from reviewing if they feel they need to.