Internet Safety Tips for Parents

1. **Do not place a computer in your child's room or other secluded place:** Keep the computer in an open common area and be aware of other computers children may be using outside of the home (friend's house, library, school etc.).

2. **Keep the Lines of Communication Open:** Use the Internet with your child. Parents should be familiar with their children's online activities. Make going online a family activity and spend time with your children while they're online

3. **Know everything that your children do online:** Read about and familiarize yourself with the on-line services that your child is using. Consider installing Monitoring and/or Filtering software. Many companies offer monitoring and filtering products that enable parents to record and/or block the Internet activities of their children. These types of programs give parents a better understanding of what their child is doing online and empowers parents to set online boundaries for their children. Filtering or Monitoring programs should never become a substitute for parental involvement and monitoring of a child's Internet use.

4. **Have a list of safety rules for your children**: Go over the rules with your child and discuss each rule to ensure that both you and your child understand. Here is an example of a list of safety rules:

Kids' Rules for Online Safety

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.
3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
4. I will never send a person my picture or anything else without first checking with my parents. I will not download a picture or program from someone without checking with my parents first.
5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do, I will tell my parents right away so that they can contact the service provider.
6. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

7. I will not give out my Internet password to anyone (even my best friends) other than my parents.
8. I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or jeopardize my family's privacy.
9. I will be a good online citizen and not do anything that hurts other people or is against the law.
10. I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology.

5. **Educate your children about the Internet, both the positives and the potential dangers.** Perform an on-line search with your child through Google or Yahoo! using search terms as "online predator news stories" or "online sexual predators" to find information about the real dangers of the Internet.

6. **Establish a password for your computer to prevent children from being online without your knowledge.** Placing a password on your computer helps to ensure that your child cannot log onto the computer without your consent.

7. **Monitor your child's email and be aware that your child may have multiple e-mail accounts**. Web based e-mail services such as Yahoo! or G-mail allow users to have numerous accounts. If your child is chatting online it is highly likely that they have an e-mail address that corresponds to their chatting user account(s). For example, Yahoo! Messenger (a chat program and service) requires that a user have a Yahoo! account in order to access their chat rooms. If your child is involved in online chatting, ask them to show you their e-mail account(s) for their particular chat service(s).

8. **Be careful when downloading or accepting images or pictures from anyone - they could be sexually explicit or contain viruses**. It is a good policy to only allow your children to accept download(s) and e-mails from people that **both** you and they know and trust in real life.

9. **Do not allow your children to go into private chat rooms without you being present.** Explain to your child that in chat rooms not everyone is who they say they are, for example a person who says "she" is a 14-year-old girl from New York may really be a 42-year-old man from California**.** One of the first things a person in a private chat room is asked is their age sex and location (typed as: "asl?"), while another is if they have a "pic" or a "cam" (webcam). They will often be asked if they wish to view someone else's webcam, which many times will show something sexually explicit. Pornography is also exchanged by online predators in some private chat rooms and will often be shared with younger "chatters."

10. **Be aware that there is an "online" chatting language involving the use of many codes**. For example, "pos" translates: parent over shoulder and "asl?" translates: what is your age, sex, and location? The code "f2f" translates as face to face. The code "cd9" stands for "code 9" and is used to convey that a parent or other adult has walked into the room. The code "MIRL" stands for "meet in

real life." Many of these codes are harmless and just for fun, but some are designed to keep parents from knowing what a child is communicating. To find a more complete list of these codes perform an internet search with Google or Yahoo! using terms like "chat slang" or "chat codes."

11. **Avoid using online screen names or email addresses that reveal personal information.** Online names often reveal information about the user. For example, the screen name "skaterboy_12_87401" indicates that the user is a 12 year old boy who likes to skate and lives in the 87401 zip code area. Other users attach birth years such as "countrygirl_1994@yahoo.com" which tells people that her birthday is in 1994. Help your child choose an online screen name that does not reveal their age, sex, or location.

12. **Keep user account profiles private**. Many e-mail and chatting services such as Yahoo! allow a user to post their personal information publicly where anyone can view. Make sure the user profile of your child is set to private.

13. **Know the Warning Signs. It is possible that your child is the target of an online predator if:**

- **Your child or teen spends a great deal of time online.** Most children who are victims of online predators spend a lot of time online, particularly in chat rooms, and may close the doors to their rooms and be secretive about what they do when they go work on their computer.

- **You find pornography on the family computer.** Predators often use pornography to sexually victimize children—supplying things such as Web sites, photos, and sexual e-mail messages as a way to open sexual discussions with potential victims. Predators **often** use photos of child pornography to convince a child that it is normal for adults to have sex with children. You should be aware that your child may hide pornographic files on disks, especially if other family members use the computer.

- **Your child or teen receives phone calls from people you don't know, or makes calls (sometimes long distance) to numbers you don't recognize.** After establishing contact with your child online, **many** online predators may try to contact young people to engage in phone sex, or to try to set up a real-world, face-to-face meeting. If children hesitate at giving out their home phone number, online sex offenders will provide theirs. Some will tell children to call collect—and then, with Caller ID or Call Display, the predators can easily determine the child's phone number. Do not allow your child to meet a stranger they have met online, in person, without your supervision.

- **Your child or teen receives mail, gifts, or packages from someone you don't know.** It's common for offenders to send letters, photographs, and gifts to potential victims. Online sex offenders even send airline tickets to entice a child or teen to meet them in person.

- **Your child or teen withdraws from family and friends, or quickly turns the computer monitor off or changes the screen if an adult enters the room.** Online predators work

hard to drive wedges between kids and their families, often exaggerating minor problems at home.

- **Your child is using someone else's online account.** Even kids who don't have access to the Internet at home may meet an offender while online at a friend's house or at another public place, even the library. Predators sometimes provide victims with a computer account so they can communicate.