Internet Safety

> **Remember, at BYU-Idaho it is expected that you live the highest standards on campus, off campus, online, and offline.**

Online Safety Tips:

- **Personal information is Personal**. Never post your phone number, address or other personal information anywhere online.

- **Make it Appropriate**. Post only appropriate pictures that reflect modest dress and behavior.

- **Know who's looking.** Potential employers and other influential people could be looking at your profile. Don't give them any reason to suspect you of being the type of person you are not.

- **Use privacy settings.** Instead of leaving your profile open for everyone to view, your privacy settings to restrict potential predators. Most sites have settings which allow more than the default privacy settings.

- **Don't just click it.** Phony advertisements and sites are designed to get your information. Do not click on links or visit sites that might be designed for this purpose.

- **Don't invite junk mail.** Be careful when filling out forms that ask for your e-mail. Many sites will send you junk mail that is hard to get rid of.

- **Buying and Selling**. When selling or purchasing items on the school Bulletin Board only deal locally. Suspicious emails from other countries should be considered fraudulent.

- **Wireless Passwords.** If you use a wireless router be sure to secure it with a password. Open wireless networks mean that you are responsible for others who are downloading or surfing via your connection.

- **Password 101.** Select a strong password to keep your accounts protected. A combination of numbers and letters to a non-word works the best. Also, it is suggested you have several passwords and don't use the same password for all of your accounts.

- **Don't get addicted.** The internet can be addictive. If you find that you are staying up late, or spending too much time on your computer, take a break and do something else.

The FTC suggests these tips for socializing safely online:
From http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

- Think about how different sites work before deciding to join a site. Some sites will allow only a defined community of users to access posted content; others allow anyone and everyone to view postings.
- Think about keeping some control over the information you post. Consider restricting access to your page to a select group of people, for example, your friends from school, your club, your team, your community groups, or your family.
- Keep your information to yourself. Don't post your full name, Social Security number, address, phone number, or bank and credit card account numbers — and don't post other people's information, either. Be cautious about posting information that could be used to identify you or locate you offline. This could include the name of your school, sports team, clubs, and where you work or hang out.
- Make sure your screen name doesn't say too much about you. Don't use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.
- Post only information that you are comfortable with others seeing — and knowing — about you. Many people can see your page, including your parents, your teachers, the police, the college you might want to apply to next year, or the job you might want to apply for in five years.
- Remember that once you post information online, you can't take it back. Even if you delete the information from a site, older versions exist on other people's computers.
- Consider not posting your photo. It can be altered and broadcast in ways you may not be happy about. If you do post one, ask yourself whether it's one your mom would display in the living room.
- Flirting with strangers online could have serious consequences. Because some people lie about who they really are, you never really know who you're dealing with.
- Be wary if a new online friend wants to meet you in person. Before you decide to meet someone, do your research: Ask whether any of your friends know the person, and see what background you can dig up through online search engines. If you decide to meet them, be smart about

it: Meet in a public place, during the day, with friends you trust. Tell an adult or a responsible sibling where you're going, and when you expect to be back.

- Trust your gut if you have suspicions. If you feel threatened by someone or uncomfortable because of something online, report it to the police and the social networking site. You could end up preventing someone else from becoming a victim.

Federal Trade Commission — www.OnGuardOnline.gov
The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

For more resources on **identity theft**, **internet fraud and scams** please visit the U.S. Securities and Exchange Division and the FBI.

http://www.sec.gov/investor/pubs/cyberfraud.htm

http://www.fbi.gov/majcases/fraud/internetschemes.htm