

The Online Safety and Ethics Initiative

Online Safety Tips

FOR PARENTS

- Teach children to use the Internet and their IT devices, such as computers and cell phones, responsibly.
- Take an active interest in how your child uses the Internet. Talk with them about who they interact with online. Try to learn what they are interested in and why.
- Be aware Websites like MySpace, FaceBook and many others provide cool places for youth to post personal information. Parents should monitor activities balancing this with appropriate levels of trust for what their children do online.
- Remind youth to not text, email, instant message or post any comment online that they would not say in-person. Also remind them that everything posted online (e.g., photos, videos and audible or text comments) remain on the Internet forever – once something is posted it can never be taken back!
- Remember that for many youth social computing is mobile computing because kids can use cell phones like a portable computer to connect online from nearly everywhere.

FOR YOUTH AND CHILDREN

- Be careful what you post to a social network. Cyber criminals, online bullies and strangers sometimes use pictures and other personal information against people in ways not easily detected or prevented. If you don't want it "out there" on the Internet and potentially used against you, don't post it!
- Never make plans to meet an online "friend" in-person who you have not already come to know as a real person.
- If you receive mean or threatening comments online, don't respond. Report the activity to your parents or another trusted adult such as a teacher.

FOR EVERYONE

- Use strong passwords and strong authentication technology to help protect your personal information. For example, **sT83bMapH** is a "strong password" because it does not spell a word or name (in any language) and does not repeat any alpha-numeric character.

- Never share your password. If you must share your password in an emergency, make sure you change it as quick as you can.
- Never open e-mails or instant messages received from unknown sources - delete them without clicking on any file attachments.
- Keep computers and all other IT devices in a safe place. Allowing someone access to any input device is dangerous!
- Keep your software current. You can prevent many problems by regularly checking for and installing updates to your operating system, browser, messaging software, and other programs.
- Consider using Internet filtering tools, but do not rely on these solely for your protection. Investigate Internet-filtering tools to complement parental supervision.
- Back-up all your data, often and in more than one way. Keep storage media safe and secure under lock and key.
- Remember that a computer or information system is only as safe as its most irresponsible user. Anyone using a home or school computer system can accidentally compromise the security of data and people who use it.