INTERNET SAFETY

Parents Handbook

SAFE SURFIN'
FOUNDATION

GENERAL GUIDELINES FOR INTERNET SAFETY

OK, parents / guardians / grandparents; Lets face it, the kids probably know more about the Internet than you do, right? Don't be intimidated! You have every right to know where your kids go online, who they talk to online and who is talking to them!

This booklet contains easy-to-follow instructions for checking your computers at home, as well as, tips and "red flags" to look for on the computer AND in your child's behavior.

BASIC RULES

Establish an open dialogue with the kids and keep it going. Show an interest in what they are doing online.

Talk to your children, no matter how young or old - remind them that people are not always who they say they are and no one they meet online is to be trusted.

Supervise all Internet-enabled devices.

Cell phones, tablets, laptops, desktop computers and game consoles all have Internet capabilities.

Get to know your child's online activities and friends.

Regularly check the online communities your child visits: Facebook, Instagram, Twitter, Reddit, Snapchat, Meetup, Tinder, Pinterest, Kik, Digg, Fark, Yik Yak, Ask.fm, and more.

Monitor what they are posting. Check out the photos they are sharing. Be aware of clues in the photo. A picture of your daughter posing in her high school's soccer uniform will make her an easy target for predators.

Teach your children to protect all personal and private information regarding themselves and their family.

Predators collect bits and pieces of information over the course of months. Many keep journals on kids they are chatting with - making notes on clues that may be released over time: where they go to school, where their parents work, what time they usually get home, etc.

Video chat should be used to stay in touch with family and friends; not chatting with strangers.

Never let your child plan a face-to-face meeting with someone they met online. If, for some reason, they absolutely must meet, then be sure you are present!

Continue to stress these basic safety rules!

Kids need to learn good online safety habits and practice them always. Remember, they are not always going to be at home when they are online. Also remember, services like Gmail and Yahoo! offer free email that they can access from any computer.

Having strong communication lines open with your kids will lessen the chance of them "sneaking" behind your back. Good discussion and parental involvement will make it easier for them to approach you for help with an online problem, should the occasion arise.

TOOLS THAT CAN HELP

- Set age appropriate filters for your child.
- Consider using monitoring software.
- Get in the habit of checking your child's online activity by viewing browser history. Be sure to check each browser and search engine on every device.
- Set time limits for online activity.
- Safe Surfin' strongly suggests NO Internet access in bedrooms. No cell phones, computers, tablets, etc.
- Limit your child's Instant Messaging or Direct Messaging contacts.
- Have a parent approved friends list.
- Use parental controls on your child's devices.
- Safe Surfin' advises absolutely NO access to chat rooms!

THE FBI reports there is 100% chance that your child will be contacted by a predator in a live chat room.
-FBI Internet Crimes Report 2012

REMEMBER, Software and other mentioned resources are NOT a substitute for parental supervision!

Be aware of your child's behavior and changes in overall attitudes. If a child has been caught up with a "friend" online that is a child predator, they will usually "groom" the child and turn the child against the parents and others close to them.

POSSIBLE DANGER SIGNS TO RECOGNIZE

Your child spends large amounts of time online, especially at night and on the weekends.

Part of a typical predator's grooming process is to be extremely controlling. They question and even threaten the child if they are offline for any undesirable amount of time - demanding to know why they were not online and where they actually were. The child will obey the predator's wishes because the child is afraid of losing their friend and confidant.

Is your child receiving phone calls from people you don't know?

Monitor call records on all devices for any unknown numbers. If a predator has their phone number, finding your home and your child's current location is easy.

Take notice if your child has new things, such as a piece of jewelry, article of clothing, Internet capable device or even a one-way plane or bus ticket.

Many predators entice their victims by sending them gifts in the mail. Video chat capable devices are often sent to a child so the predator can actually see the child while chatting. The visualization of this interaction intensifies the drive of the predator.

As part of the seduction process, it is common for offenders to send letters and pornographic images to potential victims.

Does your child turn the computer monitor off quickly or change the screen on the monitor when you come into the room?

Your child could be looking at pornographic images or having sexually explicit conversations that he does not want you to see.

Has your child become withdrawn from the family?

Electronic-sex offenders will work very hard at driving a wedge between a child and their family. Predators will accentuate any minor problems at home that the child may have - a fight about chores, poor academic performance. This is an opportunity to latch on in the form of advice, and promises of something better.

"If you were my girl, I would never make you take out the trash. You're too special for that."

CHILDREN ARE THE "IDEAL" POTENTIAL VICTIM

Naturally curious
Easily lead by adults
Need for attention and affection
Desire to defy parents, rules, expectations, etc.

Please consider talking openly with your child if you have any suspicions. Tell them about the dangers of computer sex offenders and assure them that they did nothing wrong - they will not be punished for revealing information about the online predator.

COMMUNICATION IS KEY!

What should you do if you suspect your child is being exploited?

- Review what is on your child's phone and computer - communications and images. Beware of apps like
- Snapchat that allow disappearing messages.
- Pornography or any kind of sexual communication can be a warning sign.
- Check phone contacts, call history, and caller ID.
- Block unknown contacts and speak to your phone carrier about blocking anonymous phone numbers.
- Monitor your child's access to all types of communications - text messages, video chat records, social media messages, instant message apps, chat rooms, forums, and online gaming communities.

IMMEDIATELY CONTACT YOUR LOCAL OR STATE LAW ENFORCEMENT AGENCY IF:

- Your child or anyone in the household has received child pornography.
- Your child has been sexually solicited BY ANYONE
- Your child has received sexually explicit images

Should any of the above occur, keep the device in your possession and turned off in order to preserve any evidence for future law enforcement use. Unless directed to do so by the law enforcement agency, you should not attempt to copy any of the images and / or text found on the device.

Keep talking to your children about the very real dangers that are lurking online. The digital world is always changing. Search "dangerous apps for teens" to help stay up to date and alert!

ENCRYPTION

SMART PHONE SAFETY

Before you run out and purchase a smartphone for your child, please consider the following:

- Research security settings that area available.
- Establish boundaries and rules for when and how they are allowed to use their phone AND STICK TO IT.
- Teach your child never to reveal cell phone numbers or passwords online.
- Talk to your child about the consequences of sending sexually explicit or provocative images or texts.

Let your child know that you will review cell phone records regularly, looking for inappropriate activity. Some parents hold the phone overnight and return it the next morning just to ensure they are unable to communicate late at night without you knowing.

Keep the Conversation Going

- *Ask what features they use and ask them to show you how to use them.*
- *Have you ever received a text that was rude or mean?*
- *Have you ever received a text from someone you don't know?*
- *What phone numbers do you have stored in your phone?*
- *What would you do if someone sent you a text or picture that was inappropriate?*

Sharing of Geo Data

Smartphones have GPS technology which allows the user's precise location to be pinpointed by apps and on websites. Children may share their locations unintentionally through pictures taking with their phones. These photos often have geolocation data embedded in them. Consider disabling the location services in your child's phone setting before allowing them to post online.

ENCRYPTION

ONLINE GAMING

Most game consoles allow Internet access. Don't forget to monitor your child's communication within the gaming community. Many online games have features which allow the users to create accounts and interact anonymously. Some people may take advantage of this anonymity to target children. For example, predators may send inappropriate content or use a game's communication function to arrange meeting elsewhere digitally or in-person. Online scam artists may promise virtual goods in an effort to get credit card information.

Parental involvement is critical when it comes to helping children game more safely. Take an active interest in the games that your child plays and wants to buy.

The Entertainment Software Board rates thousands of games each year. Search esrb.org

TIPS

Keep game consoles in an easy to supervise location and be aware of other places your child may be accessing games - computers, phones, friend's houses. Tell your child NEVER to give out personal information while gaming or agree to meet anyone outside of the game. Teach your child not to respond to anyone who is being rude or bullying while playing the game. Set rules about how long your child may play, what games are appropriate and who else may participate. Have your child check with you before using a credit or debit card online.
Check to see if the games your child plays have reporting features or moderators.

CHAT ACRONYMS & TEXT SHORTHAND
Understanding new cryptic code

Acronyms have always been an integral part of computer culture, and they have since spawned a new language on the Internet.
Here are some common ones to look out for:

A/S/L - Age, Sex, Location
AMA - Ask Me Anything
AITR - Adult In The Room
Banana - means Penis
CD9 - Parents Are Around
F@F - Face to Face
GNOC - Get Naked On Camera
GYPO - Get Your Pants Off
IWSN - I Want Sex Now
KPC - Keeping Parents Clueless
LMIRL - Let's Meet In Real Life
MOS - Mom Over Shoulder
NIFOC - Nude In Front Of Camera
P911 - Parent Alert
PAL - Parents Are Listening
PAW - Parents Are Watching
PIR - Parents In Room
RU/18 - Are You 18?
RUH - Are You Horny?
S2R - Send To Receive
TDTM - Talk Dirty To Me
WYCM - Will You Call Me?
WYRN - What's Your Real Name?
143 - I Love You
1432 - I Love You Too
183 - I Hate You
303 - Mom
420 - Marijuana

To learn more visit: noslang.com
                         netlingo.com
                         urbandictionary.com

Points to Remember

Understand, even if your child was a willing participant in any form of sexual exploitation, he / she is NOT at fault and IS a victim. The offender always bears the complete responsibility for his actions.

Instruct your children to:

- Never arrange a face-to-face meeting with someone they met online.

- Never post or send pictures of themselves on any online platform to people they do not personally know.

- Never give out identifying information such as their last name, home address, school name or phone number.

- Never download pictures from an unknown sources, as there is a good chance there could be sexually explicit content.

- Never respond to messages or forum postings that are suggestive, obscene, belligerent or harassing.

- Constantly remind children that just because something is posted online, does NOT make it true.

ENCRYPTION

A CHILD'S INNOCENCE CAN NEVER BE REPLACED

Moose The Family Fraternity

SAFE SURFIN' FOUNDATION

SAFESURFIN.ORG
540.855.7432