

www.Beingsmart.org



SM@RTConnections

We promote good digital citizenship by educating parents and children about the ever changing digital world; including: sexting, selfies, cyber-bullying, social media, Internet safety, self esteem, smart phone applications and digital drama.

PARENT'S RESOURCE GUIDE 2014



SMARTConnections

Table of Contents

I.	Disclaimer.....	2
II.	Mission	3
III.	Vision.....	3
IV.	Contact Us	3
V.	History	4
VI.	Local Resources.....	5
VII.	Online Resources	6
VIII.	Cell Phone Providers	7
IX.	Internet Providers.....	9
X.	Safety Pledges:.....	11
XI.	Digital Citizenship Pledge	11
XII.	Online Safety Tips.....	12

Disclaimer

All information contained in this parent resource guide is the property of the organization to which it is referenced. Information for services offered is taken directly from the organization itself or the organization's website which is listed along with the information provided. **SMARTConnections** has simply placed this information in a convenient location for parents to access quickly.

Information contained in this parent's guide is current as of the date of publication. Please check the referenced websites associated with the information for the latest information and or services offered.

SMARTConnections does not endorse nor support any specific organization listed within this guide; nor does any organization support nor endorse **SMARTConnections** unless specifically mentioned.

Mission

- i** Our mission is to educate parents, teens, children and the community how to be responsible Digital Citizens while online, as well as, the possible dangers of the Internet and social media with an emphasis on sex-ting awareness and prevention.

Vision

- i** Our Vision is to help educate the Henderson community, southern Nevada and all users of cyber-space on how to be good Digital Citizens while online. We partner with other organizations to fill the holes in education and prevention related to Internet safety, sexting awareness, and good online Digital Citizenship.

Contact Us

- i** Would you like us to do a presentation for your business, organization, or school? Would you like to learn more information on the services we provide? Please check us out at:

www.beingsmart.org

[www.Facebook.com/beingsmart.org](https://www.facebook.com/beingsmart.org)

[http://instagram.com/smartconnections](https://www.instagram.com/smartconnections)

Need more information please contact us at:

chris@beingsmart.org or call (702)530-1344

****Note that we are run by volunteers and we make every effort to reply to your inquiry within 24 hours. ****

History



SM@RTConnections was born through a partnership with the Henderson Chamber of Commerce- Leadership Henderson program, and is the Leadership Henderson 2014 class project.

The class of 2014 in partnership with the Henderson Community Foundation, and the Henderson Police Department created **SM@RTConnections**; which was the vision of Chris Holman a 2005 Leadership Henderson Graduate and a current Investigator with the Henderson Police Department.

In August of 2009 Chris Holman was moved to the Henderson Police department's Computer Crimes unit. During his assignment in Computer Crimes it became very clear to Chris that more education was needed to prevent self-produced child pornography, more commonly referred to as "sex-ting" by the media, and popular teen culture.

In 2010 Chris began to present Internet Safety, cyber-bullying prevention, and social media awareness classes to schools, and civic organizations.

In 2013 Chris was approached by the Henderson Community Foundation and the Leadership Henderson program to submit the **SM@RTConnections** concept to the 2014 class for consideration. Chris presented the concept, with the help of a Family who had personally experienced the devastating effects that "sex-ting" can have.

The Leadership Henderson class of 2014 chose **SM@RTConnections** and is working hard to make this the best program possible.

SM@RTConnections partners with other organizations to fill in the holes in education and prevention as it relates to Internet safety, social media awareness and "sex-ting" prevention. Together the community can make a difference in the lives of those affected by poor digital citizenship choices.

SM@RTConnections currently offers its services free of charge. However, donations are gratefully accepted. Donations can be made at www.beingsmart.org and follow the Donate link.

SM@RTConnections is a component fund of the Henderson Community Foundation, a recognized 501(c) 3. Any contribution you make to **SM@RTConnections** may be tax deductible to the extent allowed by the IRS.

Local Resources

If you or someone you know are a victim of an online predator please contact your local Police Department in Southern Nevada:

National Center for Missing & Exploited Children

(800) THE-LOST

(800) 843-5678

www.missingkids.com/cybertipline

Henderson Police Department

(702) 267-5000

www.cityofhenderson.com/police

North Las Vegas Police Department

(702) 633-9111

www.cityofnorthlasvegas.com/departments/police/police.shtm

Las Vegas Metro Police Department

(702) 828-2906

www.lvmpd.com

Boulder City Police Department

(702) 293-9224

<http://www.bcnv.org/?q=police>

Nevada Child Seekers

<http://nevadachildseekers.org>

(702) 458-7009

Rape Crisis Center

www.rcclv.org

(702)366-1640

United Way of Southern Nevada

www.unwsn.org

(702)892-2300

Online Resources

Common Sense Media	www.common sense media.org
Net Smartz	netsmartz.org
Connect Safely	connectsafely.org
Kids in the Know	Kidsintheknow.ca
Child Lures Prevention	childluresprevention.com
Web Wise Kids	webwisekids.org
Get Net Wise	Getnetwise.com
Safe Kids	Safekids.com
I-SAFE	isafe.org
Cyber Angels	cyberangels.org
Wired Safely	Wiredsafely.org
Child Net International	childnet.com
Family Online Safety Institute	fosi.org
In Hope	inhope.org
Cyber bullying Research Center	Cyberbullying.us

Cell Phone Providers



Smart Limits for Wireless

- Allows you to block unwanted calls and texts (up to 30 numbers).
- Allows you to block or limit the purchase of apps.
- Allows you to restrict texting, browsing and outbound calling during specified times of the day.

AT&T Smart Limits plan is \$4.99 per month per user.

For more information:

<http://www.att.net/smartcontrols-SmartLimitsForWireless>



Sprint Mobile Controls

- Easy to read dashboard allows you to monitor your child's phone usage, and to access the phone's complete setup.
- See who your child is talking or texting with, and at what times.
- Establish an "Allowed list of phone numbers that can call or text your child.
- See what apps your child is downloading to their phone.
- Sprint Mobile Controls is compatible with Android devices at a cost of \$4.99 per month, per device. Free trial is available.

Use your phone's GPS to locate family members with real-time interactive satellite maps including street addresses and landmarks.

For more information:

http://shop.sprint.com/mysprint/services_solutions/details.jsp?detId=sprint_guardian&catId=service_safety_control&catName=Safety,%20Security%20and%20Control&detName=Sprint%20Guardian#



Family Allowances, managed through “My T-Mobile”

- Allows you to manage minutes, messages, and downloads for all lines on your account.
- You can set “Always Allowed” and “Never Allowed” numbers to restrict calling and texting.

Allows you to manage phone usage during certain times of the days.

For more information:

<http://support.t-mobile.com/docs/DOC-1725>



Security Family Base

- Provides a dashboard to monitor your child's wireless usage. Know when and how your child used their phone.
- Allows you to set limits on data, voice, and messaging usage.
- Allows you to see all application installed on your child's device as well as the frequency of use.
- Allows you to view all contact you child has made with the ability to add trusted contacts and block unwanted contacts.
- Allows you to limit or restrict the phone's usage on demand.
- Locate your family members using the phone's GPS (\$9.99 per month per account).
- Allows you to block the download or set the permissions on downloading of apps.

Set Content filters to make sure your child can only access age appropriate material.

For more information:

<https://wbillpay.verizonwireless.com/vzw/nos/safeguards/safeguardLandingPage.action?intcmp=INT-MVZSAFEGUARDS>



Parental Controls



- **How do browsing modes in Parental Control work?**

With the Parental Control browsing modes, you can define browsing times and web sites that are suitable for your teenagers and small children. You can give your teenagers more freedom to browse the Internet while having tighter restrictions on your small children's online activities. You can create and set up the Parent, Teenager, and Small Child browsing modes either with a Start-up Wizard, during the installation, or later on the Parental Control page.

The Small Child browsing mode is active after you have installed the product or restarted the computer.

- **When the Small Child mode is active:**

Anyone using the computer can access only those web sites that you have specifically allowed. Access to the Internet is allowed only during the scheduled time. All the web sites that you have allowed are listed on Parental Control Start Page that opens in the browser when the Small Child mode is active.

- **When the Teenager browsing mode is active:**

Anyone using the computer can access all web sites, except those that contain restricted or unwanted content. (IE; drugs or adult material)

Access to the Internet is allowed only during the scheduled times.

For more information contact your service provider or visit this website:

<http://internethelp.centurylink.com/internethelp/security-fsecure-v9-controls.html>



High speed security solution

With Cox High Speed Internet, you get complete PC protection for your entire family with Cox Security Suite. Cox Security Suite powered by McAfee™, can easily be downloaded and managed from My Connection. It gives you the latest features in Internet security, and it's included free with your high-speed service. A standout feature for many families is the ability to manage, monitor and protect your children's online experience.

Safeguard your family with parental controls

Parental Controls allow you to set filters on your computer and manage your children's internet experience. You can restrict certain sites, images, use and access at certain times of the day. Customizable controls for each user name is also available. You can see what sites your children have accessed or attempted to access while they were online.

Manage your kids' Internet use

- Parental Controls – Apply adjustable rules to block inappropriate sites and limit online time.
- Surf Report – Check sign-in times by user, attempts to access forbidden sites and total online time.
- Improved Summaries – See and print on usage report for all your kids.

There are a number of excellent family internet sites available to further assist you in guiding your family through a safe internet experience. The first we'd recommend is our own Take Charge site. Here you'll find the latest Internet safety tips, advice on how to communicate with your kids, and links to Internet-friendly programming. You'll find all this and more at www.cox.com/takecharge .

For more information:

<http://www2.cox.com/myconnection/learn/safe-and-sound/protect-family-online.cox>

Safety Pledges:

i "House pledges" or "acceptable-use policies" can help provide clear guidelines for safer Internet use. www.NetSmartz.org recommends using the "Internet Safety Pledge" to promote safety discussions and create safer boundaries.

Internet Safety Rule

1. I will tell my trusted adult if anything makes me feel sad, scared, or confused.
2. I will ask my trusted adult before sharing information like my name, address, and phone number.
3. I won't meet face-to-face with anyone from the Internet.
4. I will always use good "net-iquette" and not be rude or mean online.

Real-World Safety Rules

1. I will always check first with my parent, guardian, or other trusted adult before going anywhere, helping anyone, accepting anything, or getting into a car.
2. I will take a friend with me when going places or playing outside.
3. I will tell people "NO" if they try to touch or hurt me. It's OK for me to stand up for myself.
4. I will tell my trusted adult if anything makes me feel sad, scared, or confused.

NetSmartz has multiple age based pledge samples and guides available online at:

www.netsmartz.org/resources/pledges

Digital Citizenship Pledge

I will practice legal, safe and kind behavior while on the Internet and Social media. I will protect my **Name**, **Identity**, and **Reputation** while online. I will be a good Digital Citizen.

Name: Anything posted on the Internet is not private. I will be careful when posting information about me online. Including my Name, contact information, school, friends, relatives and pictures of me. I will check my privacy settings on social media accounts with my parents.

Identity: I will protect my online identity. I will be real and respectful. I will not create fake profiles or pretend to be older than I really am. I will protect my password.

Reputation: How I act, what I post, and what I share online will form my online Reputation. I will discuss what is acceptable to post online with my parents or guardian. I will post clean pictures, and respect myself and others while online.

Cyber-bullying: I have the right to use technology without being threatened, harassed or pressured by anyone. I will tell a trusted adult if anyone makes me feel that way. I can report the person bullying me online and/or block them. I will not respond to the person online.

Social media stress: If I feel stressed out online I will "**UNPLUG & GET A HUG**". It's ok to log off.

Digital Drama: If I witness digital drama I will remember... "**When there is drama, tell your Mama**". I will tell a trusted adult if I feel stressed or witness digital drama.

Online Safety Tips

Clear, simple, easy-to-read house rules should be posted on or near the monitor. Create your own computer rules or print the Internet safety pledge. The pledge can be signed by adults and children and should be periodically reviewed.

Look into safeguarding programs or options your online service provider might offer. These may include monitoring or filtering capabilities. Many of these services are free.

Always read a website's privacy policy before giving any personal information. Also make sure that a website offers a secure connection before giving credit card information. (https) The "s" is for secure. You can also look for a padlock icon in the bottom corner of the site.

Websites for children are not permitted to request personal information without a parent's permission. Talk to children about what personal information is and why you should never give it to people online.

If children use chat, e-mail, or social media programs or applications make sure you talk to them about never meeting in person with anyone they first "met" online.

Talk to children about not responding to offensive or dangerous e-mail, chat, or other communications. Report any such communication using the website or applications reporting functions. If you are not sure how to do that consult your local law enforcement agency.

Do not delete the offensive or dangerous e-mail; turn off the monitor, and contact local law enforcement. Deleting the offensive material or communication may destroy valuable information that could aid law enforcement in identifying the source of the communication.

Keep the computer in the family room or another open area of your home. Position the monitor so it faces the center of the room, and can easily be seen throughout the room.

Let children show you what they can do online, and visit their favorite sites. Ask them what they use the sites for. Watch them use the sites and ensure you know how they work before letting your child play alone.

Have children use child-friendly search engines when completing homework. Turn on web content filtering to ensure the ratings of websites are age appropriate. (See parental controls)

Be aware of any other computers your child may be using. Many tablets, smart phones, game consoles, and hand held games can also access the Internet.

For parents with younger children, Internet accounts should be registered with the parent's email accounts so the parent has the primary screen name, controlling passwords, and ensure age appropriate restrictions are in place.

Children should not complete a profile for a service provider and children's screen names should be nondescript so as not to identify that the user is a child.

Talk to children about what to do if they see something that makes them feel scared, uncomfortable, or confused. Show them how to turn off the monitor and emphasize that it's not their fault if they see something upsetting. Remind children to tell a trusted adult if they see something that bothers them online.

If you suspect online "stalking" or sexual exploitation of a child, report it to your local law-enforcement agency. The National Center for Missing & Exploited Children (NCMEC) has a system for identifying online predators and child pornographers and contributing to law-enforcement investigations. It's called the CyberTipline®. Leads forwarded to the site will be acknowledged and shared with the appropriate law-enforcement agency for investigation.

Consider using filtering or monitoring software for your computer. Filtering products that use white listing, which only allows a child access to a preapproved list of sites, are recommended for younger children. Net Smartz does not advocate using filters only; education is a key part of prevention.

Smart phones, laptops, tablets, and portable gaming consoles all come standard with web cameras now. Devices with cameras need to have special considerations made about where and when the devices can be used. Devices with cameras should never be allowed in the bathroom. Understand the risk of allowing devices with cameras in the bedrooms.

Many new viruses, spyware, and Trojan horses can infect a portable device with software that can allow the "Spy" to activate webcams without the user knowing that they are on. Consider putting a piece of black tape over cameras that are never used, close the lid on devices when not in use, and never position the camera in areas where people are sleeping, changing, or bathing. Ensure anti-virus software is installed and up to date.

Smart phones can hold many applications which can be used for any number of things, such as: games, pictures, texting, social media, and surfing the Internet. Some applications are designed to hide other features. Many calculator applications can hold secret pictures, movies, and music. Some applications are secret folders which can conceal other applications. Make sure you know what is on your child's smart phone and tablets, and click each one to ensure they do what you expect them to do. If there is more than one calculator application or vague applications, ask your child about them, and search the app store or web to find out more information.

Remember:

- 1. You don't have to respond to people you don't know or who make you feel upset.**
- 2. You can report and/or block cyber-bullies and predators.**
- 3. You can log off if you feel stressed or upset.**
- 4. Don't delete evidence if you are going to file a police report.**

Safety tips provided by netsmartz.org/resources/pledges and
www.beingsmart.org



SM@RTConnections

Thank You!