Parents:

Middle school students struggle to make appropriate decisions with social media and need direct and frequent guidance and monitoring to make appropriate choices. Many times students are given access without adequate training on how to use the technology appropriately. We want to encourage parents to take an **active role** in teaching their children healthy online behavior. The following list are a few of our recommendations for families:

1. Decide what level of technology access is appropriate for each child in your family. Don't blindly give your student a phone with a full data plan without appropriate training, supervision, restrictions, and guidance. Consider gradually giving students more phone/internet/app privledges as they mature and demonstrate responsible behavior. Set appropriate consequences if students fail to abide by family policies.
2. Regularly check and monitor apps and text messages on your student's phone. Set up restrictions on your student's phone and explore options that allow you to monitor your student's social media and internet activity. Start restrictively and gradually give your student more privledges if they use technology appropriately.
3. Have frequent discussions with your student regarding what is appropriate to post on social media and how to respond to inappropriate posts, texts, and requests. **Discuss** what information is appropriate to make public. **Ask** your student what they are seeing on social media. **Guide** them in how to deal with negative posts. **Encourage** them to "unfriend" someone who is being nasty or sending harassing messages.
4. Monitor the "friends" or "followers" on your student's social media accounts. Many times students blindly accept strangers as "friends."
5. Require your student to set all social media accounts to "private" so only accepted friends can view posts. Check on these settings frequently—many times app updates change default privacy settings.
6. Set up "no cellphone" times such as mealtimes, bedtime, and family time. Consider setting up guidelines that all family members follow.
7. At bedtime, have a designated spot for cellphones (kitchen counter/parent bedroom) to keep phones out of your students' bedrooms at night.
8. Do not feel guilty for "invading the student's privacy" by monitoring cell phone activity. Parents always ask questions --"Where are you going?"..."Who are you going with?"... "What are you doing at their house?" Parents even check to see if the student is where they said they would be or check out who their student is actually hanging out with. In this digital age, it is important to do the same with cell phones and internet activity as your student grows and develops through middle school.

We have included several documents to give parents a place to start for parents to understand and control their student's online activity.

- **Internet Filters and Monitoring Tools**—A list of proactive Apps and filters for online safety
- **Common Sites/Apps used by Teens**—Not an exhaustive list, but a good place to start to educate yourself on some common apps teens are using.
- **Technology Contract**—This is a sample technology contract for parents to consider with their student. This contract is posted on the CMS guidance site—feel free to download and edit it any way you see fit if you feel that a contract is a good option for your family. If you use a contract, use it as a teaching and discussion tool rather than it just being a piece of paper that is signed. Take time to review it and discuss it regularly with your student.

# Internet Filters and Monitoring Tools

The following list provides parents a starting point for increasing their own understanding and control of their child's online activity. The school is not recommending any of these resources in particular but hopes to provide parents resources proactively. Parents are encouraged to independently explore which of these tools may best allow them to teach digital citizenship to their children and develop a family plan for utilizing social media and the internet responsibly.

At the very least, parents should initiate ongoing conversations about how their children are engaging with technology while periodically revisiting how those social media sites are being accessed and utilized by their children. Parents need to be intentional about teaching appropriate online behavior in order to reduce the potential negative impact of social media and to ultimately keep their children safe physically, socially, and emotionally.

## Proactive Apps for Parents:

1. **KnowBullying** is a free app that provides parents directed age-specific conversations starters for their children, regular reminders, social media strategies and tips, and suggestions on how to help their children deal with difficult social situations.

2. **Halt** is a social media monitoring tool that allows parents to see all posts, pictures, tweets, and updates of their children's social media accounts on a variety of networks including Facebook, Twitter, and Instagram. Registration requires user/child's log in info. Parents can use this as a springboard to educate children about responsible online behavior, step-in to delete inappropriate posts, or document online harassment.

3. **AppCertain** is a free app that allows parents to receive notifications about the applications installed on a child's device(s). It will share a synopsis of the app, in-app purchase capabilities, functions, risks, age-appropriateness, etc. The goal is to help parents know what the apps are used for, which enables parents to have informed discussions with their children about these apps.

4. **TeenSafe** allows parents to monitor their child's cell phone activity, including sent and received text messages (even deleted texts), call and web history. However, the feedback is not real-time. There is a Live GPS Location Monitoring feature. Parents need to know their child's Apple ID and password to set up an account. One free week trial is available and then, for continued service, users pay a monthly fee.

## Online Safety:

1. Some **routers and search engines** have parental controls built in and simply need to be programmed. These sources can provide additional support:
   - **Open DNS** offers free, customizable parent controls for an array of internet-connected devices (computer, gaming consoles, phones, friend's devices) being used in the home. Parents can gain insight to which websites are being visited on their home network. Additional services can be added with a yearly subscription.
   - **Mobicip** is a free content-filtering browser that allows parents to remotely manage settings, monitor internet and app usage for multiple users. Parents can receive alerts when content is blocked on a protected device. Various levels of "restriction" can be applied to different profiles (ex: Elementary, Middle, High, or No Filtering) as well as time limits. Detailed reports of browsing history are available.

2. Consider enabling **restrictions** within the "settings" of your mobile devices. Periodically check **privacy** settings within apps as they often change with updates.

3. **OnGuardOnline.gov** is an excellent parent resource that providing tips for protecting kids online, teaching tools and parental control options. Find more resources like this on the NACS website under Bullying Prevention.

# Common Sites and Apps Used by Teens

## SOCIAL NETWORKING:

**Facebook** is the top social network on the web as it is used by more than 1 billion people each month. You can access this service using an app on a mobile device or internet service for a computer. People set up a profile and accept "friend requests." There is a timeline to post events and share "status updates." Certain groups can be set up as private or public. Users can be referenced in someone else's text or picture (tagged). Teens are moving away from fb because many parents and grandparents are on the site. Officially, individuals should be 13 years of age to create an account but students in elementary schools report using this social networking site.

Like Facebook, **Twitter** is a social network centered on microblogging with a 140-character text limit. An uploaded picture or text message is called a "Tweet." The public can "follow" friends, celebrities, causes, businesses or tv shows. You can "tweet" live during a show by using # (hashtag). Students report concerning "subtweets," which are comments intended for someone to see without mentioning their username, usually with a derogatory tone.

**Ask.fm** is another popular pre-teen social networking website where users can ask other users questions. Users have to create an account to leave or receive comments. Ask.Fm is different than Facebook and Twitter because users can ask questions or leave comments anonymously. However, there is the option for users to not receive comments unless a sender identifies himself. This has been a popular venue for cyber-bullying.

**Whisper**, an app that lets people broadcast their thoughts with the world anonymously, estimates that 90% of its population is 18 to 24 years old. This app appeals to a younger demographic who report having a "strong desire to share thoughts more freely without worrying about online identities and accountability" – unlike Facebook and Twitter. It is predicted that users will leave Facebook and Twitter for this social networking site. Messages and photos do not self-destruct after they are read (like SnapChat). Whisper does automatically filter for trigger words or for proper names in an attempt to create a "safe place" for users. However, pictures of peers can still be posted without names attached.

**Tinder** is a simple-to-use dating app. The app finds a person's location by GPS then links to his/her Facebook profile to access user information - first name, age, photos (by user choice) and some Facebook preferences. It will then find potential matches near the user's physical location. Users scroll through pictures of "matches" selecting "like" or "nope" to other user profiles. Tinder is well known for allowing users to judge other users based on appearance and criticized for facilitating "hookups."

**Yik Yak** originated similarly to Facebook on a college campus and intended for college-age users but is becoming increasingly popular among high school students. This social media app can be considered a "local, virtual bulletin board." Posts or comments ("yaks" up to 200 characters) are made anonymously and can be viewed by fellow "Yakkers" in a 10 mile radius. Users don't have a photo or avatar distinguishing themselves. Posts are "upvoted" or "downvoted," allowing users to earn reputation points. High potential for cyber-bullying, sexually explicit content, and derogatory language.

## PICTURE SHARING:

**Tumblr** is another form of microblogging, but unlike Twitter, it is heavily influenced by image sharing. You can follow other users and be followed back. "Reblogging" and "liking" is a popular way to interact and to see how many followers you can attract. Users can make their site private so others cannot see it without becoming a follower by permission. Features are accessed from the "dashboard." Tumblr is noted by critics as having a sizable amount of pornographic content.

**Instagram** is a photo app designed for the iPhone and a mobile social network. Users take a picture with their phones and then edit instantly or apply photo filters. You can follow other Instagram users to view their photos and interact by "liking" their photos or commenting on them. It is easy to share your photos on other popular social networks. GPS attaches to photos.

**SnapChat** is a popular app among teens and younger users. It allows users to take a photo or a video and chat back and forth with somebody through the app. The photo or video self-destructs automatically in just a few seconds (1-10 seconds) after the recipient has viewed it. However, the pictures can be captured by screenshot or downloading. A writing tool can be used to embellish a photo. It is possible for someone to take "screen-shot" of the received photo. There's been quite a bit of controversy surrounding how teens are using this app for sexting and cyber-bullying.

## VIDEO SHARING:

**YouTube** is used mostly for video sharing and revolves entirely around video production, vlogging, movie-making and music sharing. Individuals can upload their own videos, or view others. Users are able to subscribe to "channels" that are videos from the same source. The terms of service state that offensive content such as sexually explicit material, and types of abuse, are forbidden. However, the video must be flagged as inappropriate by other users for the site management to become aware and remove it.

**Vine** is a video creation app owned by Twitter where all the videos are 6 seconds or less. The videos, or "vines," play in an endless loop. Twitter guidelines state that users are allowed to post pornographic images on their sites. Therefore, Vine has a 17+ rating but there is no age verification when creating an account. All profiles are public.

## INSTANT MESSAGING:

**Kik** Messenger is a free app-based alternative to "old-fashioned" texting as well as a social networking app for mobile devises. It only needs a Wi-Fi connection or data plan to send and receive messages so a phone texting plan is not necessary. Kik requires users to register a username as a form of identification. The service is used for sharing text, pictures, voice messages and sketches. One criticism is that adult-content can easily be shared by linking to other sources, such as YouTube. Safety and privacy issues can also be of concern.

# Technology Contract

Created by Paige Clingenpeel, L.M.H.C.
trendsandteens@remedylive.com
www.TRENDSandTEENS.com
2014

*I understand that having any device is a gift not a right. Having a phone, computer, and Internet access is a partnership with my parents. I am allowed to question and suggest changes to the rules, but in a respectful way. I understand that as I prove myself responsible that I will be allowed more privileges; if I prove myself irresponsible I will loose privileges. And I understand that both of those options are my choice as shown in my behavior.*

## Cell Phone:

- I will plug my phone in my parent's room by _____ on school nights and _____ on weekends
- I will always answer or respond to the phone when my parents call or text
- I will not use my phone during meals, school, family and friend time, and while interacting with others
- I will not use my phone to talk or text while driving. I will either turn my cell off or on silent, while placing it in the glovebox or in the back pocket of the driver's seat. If I need to text or call someone then I will park my car in a safe location like a gas station or parking lot.
- I will not use my phone when people are talking to me in person. Instead I will make eye contact, respond with words not just grunts and shoulder shrugs.
- I will not hide or delete information on my phone (text, pictures, call log, emails, etc)
- I will not download any app, music, movies, or games without talking to my parents first
- I will remember that texting is not the best way to talk to my friends or family, and instead will have majority of my conversation in person or talking on the phone. If I text them more than 3 times then I need to just call them.

## Computer/Internet Use:

- I will be off the Internet by _________ on school nights and __________ on weekends.
- I will not look at, listen to, or talk about things that I wouldn't want to show my parents (such as pornography, graphic/violent, inappropriate language, etc)

- I will never give my information such as name, address, school, phone number, etc to anyone online, even if I believe the person to be safe. If I believe the person or website is safe, I will ask my parents prior to providing the information.
- I will never buy anything online without talking with my parents first
- I will not join a social network without my parents permission

## General Technology:

- I will never text, email or say anything that I would not say in person, or in the presence of an adult. Because I know that words are powerful and could hurt others.
- I will never send, forward or respond to a threatening, abusive, or provocative message. Instead I will talk to my parents or trusted adult to discuss ways to respond to the situation.
- My parents will always have access to all my accounts, email, social network, iTunes, etc
- I will never create an account that I keep as a secret from my parents
- I will let my parents read any text, email, call log, etc whenever they ask. I'm allowed to be frustrated at the request, but I won't be disrespectful.
- If my phone, computer or other device is damaged, lost or broken, I am responsible to repair or purchase a new one
- I will never use any device to lie, deceive or manipulate others. This means I will never lie about my age, or act like another person.
- I will never take, send, or forward a picture of myself or others that I wouldn't want my parents to see. Because I know that uploading or sharing a picture of a person that is provocative is now seen as child pornography and is punishable by jail and labeled as a sexual offender.
- I understand my parents can add and change the technology contract at any time

My Signature & Date:______________________________

Parents Signature & Date:_________________________,_____________________________