

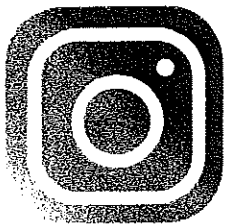
# APPLICATIONS TO WATCH



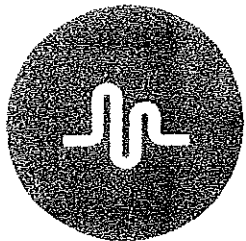
**Twitter** - Service that enables users to send and read short messages called "tweets". Registered users can read and post tweets, but those who are unregistered can read them.



**Facebook** - A social networking website that makes it easy to connect with friends and family online. Currently the largest social network with over 1 billion users worldwide.



**Instagram** - An online photo sharing and social networking service that allows its users to take a picture, apply a digital filter to it, and share it on many social networking services.



**Musical.ly** - A social network app for video creation, messaging, and live broadcasting. Users can create 15 second to 1 minute videos and choose music to accompany them.



**Snapchat** - Users set a time limit for how long selected recipients can view their photos, and videos, after which it will be deleted. In actuality, it is very easy to save incoming messages and images.

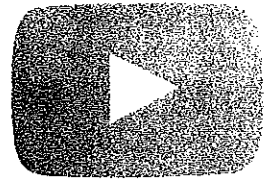


**Tinder/Blindr** - Dating and rating sites based on location. Users upload pictures and personal information to be seen and judged by those located nearby.

**Kik/Whatsapp** - Messaging apps that anyone can use for one-on-one and group chats. There are ways to register without phone number verification on both of these applications..



**Youtube** - Global video-sharing website that allows users to upload, view, rate, share, and comment on videos. Non-registered users can also watch content.

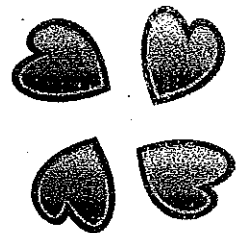


**Omegle/ Chat Roulette** - Free online chat website that allows unregistered users to chat by randomly pairing users in one-on-one video sessions where they chat anonymously.

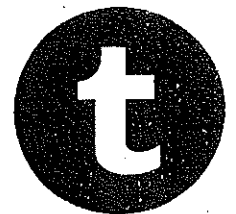


*Chat Roulette*

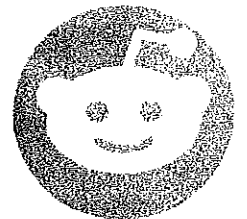
**4chan** - An imageboard website where users post anonymously into various topic boards. Registration is not possible, except for staff members. Inappropriate content can be easily accessed!

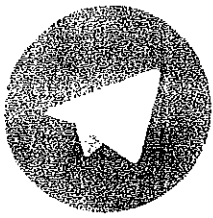


**Tumblr** - This is a popular microblogging platform but it is also a highly risky place for kids/teens. The content that is posted here is usually unsupervised and known to contain pornography.



**Reddit** - Registered members submit content to the site such as links, text, and images, which are then voted up or down by members. Posts are organized by topic into "subreddits".





**Telegram** - Telegram accounts are tied to telephone numbers. A user can set up an alias that allows them to send and receive messages without exposing their phone number.

**Whisper** - Allows users to post and share photo and video messages anonymously, although this claim has been challenged with privacy concerns over Whisper's handling of user data.



**ASK.fm** - A global social networking site where users create profiles and can send each other questions. It is a form of social media that encouraged questions to be submitted anonymously.

**WeChat** - Users can send previously saved or live pictures and videos, namecards of other users, coupons, lucky money packages, or current GPS locations with friends either individually or in a group chat.



## HOW CAN I KEEP MY CHILD SAFE ONLINE?

- Start by talking with children about their online activities. The sooner you do this, the more normal it becomes.
- Teach your child that what is said online is not sacred, protected, or secret. It is NOT their diary, it's the public internet, even if said on a private page.
- Set up Google Alerts to monitor mentions of children's names on the web. (<http://www.google.com/alerts>)
- Friend them on Facebook and monitor their privacy settings so you are able to "spot check" their profile and activity.
- Prohibit your child from using multiple screen names and accounts. This could be a warning sign that your child is abusing other teens. Be nosy.
- Start from the beginning: just like anything else, kids need to learn from YOU how to be a good "digital citizen". You wouldn't toss them the keys for your new car at 16! Teach them how to act online.
- Set up guidelines for using the internet and social media. Kids can get around many of your blocks and filters. Check in on them.
- Whenever possible, allow them to use the computer in a central location that is supervised until they earn your trust. After this, you still need access to all of their accounts and apps on their phones and tablets. Look up the names of the apps and their purpose.
- Monitoring software can be utilized, but keep in mind that most teens are now using their phones as a means of communication with social media.
- Teens frequently share passwords as a sign of friendship and trust. Talk to them about why this is dangerous, and remind them that relationships can quickly change, leaving them vulnerable to attack. If you wouldn't give them your ATM pin, don't give them your passwords.
- Never take people at their word over social networking if they are not known to you. They know very well how easy it is to create a persona.
- Talk to teens about their reputations and online identity. How you treat people matters, both online and offline.
- Remind students (who have their own accounts and cell phones), on a regular basis about the dangers of sending inappropriate messages and texts.