

Student Online Safety





"It isn't that teens are dedicating themselves to social media *instead* of living their lives. It's that social media is their preferred tool for communicating, sharing, and all the other things teens do as they grow into young adults"





When the cordless phone became a household item, teens spent hours in their rooms talking to their friends.

The Internet in general, and social media in particular, is simply a better tool, allowing teens to talk to all their friends, see their updates, and keep in touch in real-time



Cell Phone Ownership

- Ages 6 to 9 22%
- Tweens (10 to 14) 60 %
- Teenagers (15 to 18) 84 %

**Data from PEW research group





- Most teens are on their phones all the time in school, in bed at night, when they go to the bathroom, while you are trying to talk to them, and while they are trying to do their homework
- They are in instant access with each other all the time
- There are virtually no enforceable parental controls short of depriving a child of a phone which then subjects them to rejection from their real and virtual friends.
- The popularity contests of childhood are online now and revolve around how many "likes" you get. A low number of "likes" typically translates into low social status, and possible shaming and bullying. A high number of "likes" translates to popularity and the pressure to sustain your status. Netflix Black Mirror (episode: Nosedive)









- Chat Rooms 1994
- Sixdegrees.com 1997 (3.5M Users)
- Wikipedia 2001
- Friendster 2002
- MySpace 2003
- Harvard version of Facebook 2004











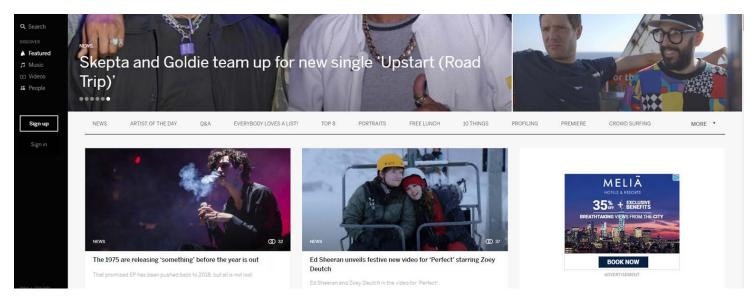








Do you recognize this social media site?





Terms and Conditions

- Agree to allow the sale of your information to third party vendors
- Your photos are now the property of FB, Instagram, etc..
- Agree to allow them to track your geographical location and sell it to vendors
 - <u>iOS</u> Privacy => Location Services (toggle off/on per app)
 - Android App Drawer => Settings => Location Settings
- Your personal information has value / Are you getting enough back from the app?



Your Digital Footprint

- College Admissions & the Military: College admissions officers can and do read your teen's online profile.
- Scholarships: Scholarships often ask applicants to share their social media profiles as part of the process in applying online.
- **Sports:** Is your son or daughter planning on playing sports in college? Recruiters and coaches surely will want to know about your teen's conduct on social media.
- Employers & Internships: Employers will Google your kids. The difference
 between your son or daughter and another applicant could be their digital footprint.



KIK



Kik is a smartphone messenger application that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos and more – all with the app.

Unlike many other smartphone instant messengers, which are based on a user's phone number, we use usernames to identify our users. By using usernames instead of phone numbers as the unique identifier on Kik, users' personal information like cell phone numbers and email addresses are never shared by Kik.

The "Block" feature allows our users to block all contact with another user, without revealing to the other user that they've been blocked. Blocking someone means that messages from this user won't appear in the blocker's conversation list, and all previous conversations with this person will also be hidden. The blocked user's username will no longer appear in the blocker's list of contacts in Kik.

Students like this app to create anonymous texts to anyone that could be inappropriate.





Snapchat is a photo messaging application allowing users can take photos, videos, add text and drawings, and send them to a predetermined set of recipients. Users set a time limit for how long recipients can view their Snaps (messages) from 1 to 10 seconds, after which they will be hidden from the recipient's device and deleted from Snapchat's servers.

Snapchat is designed so that all photos and videos will disappear after a predetermined amount of time set by the sender. However, users have negotiated ways to keep photos after their intended time set. One of the primary ways Snapchat users keep photos is through taking a snapshot. A screenshot is when the user makes their own copy of the photo by taking a photo of their screen while the snap is showing. In addition, there are applications available that will circumvent Snapchat's deleting system and save photos or videos permanently.

Many teens use this application, the main demographic of Snapchat users are between 13 and 23 years of age. That is why it is important to stress to children and teens that once an image is online, there is no getting it back. Children need to be mindful of who receives their messages, what those messages contain and how it could be used to hurt them. Posting a child's pictures on any site could put them at risk for victimization.

Crimes that have been used are; threats, harassment, sexting, and drug dealing.



INSTAGRAM



Instagram is an online mobile photo-sharing, video-sharing and social networking site that enables users to create an account and upload pictures or videos and share them on several other social networking sites such as Facebook or Twitter.

You can adjust your privacy settings to private on the account.

Monitor who is following you and make sure it is not strangers.





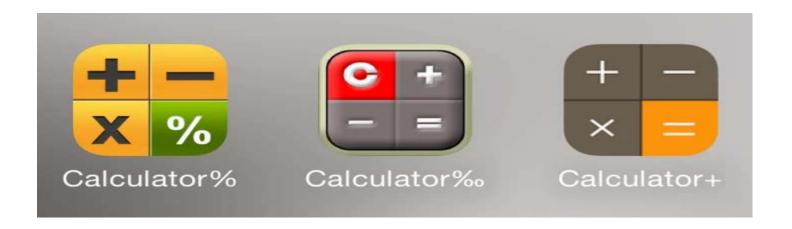
PARENTAL TIPS

- Do you know your child's password?
- Do you know all the social media applications on their electronic devices?
- Periodically check their browser history for inappropriate content.
- Check their privacy settings (restrictions, data usage, privacy)



HIDDEN APPLICATIONS

Hidden app's may look innocent but are used to hide inappropriate content or pictures. Typically a password is required to open the application. The applications we have seen look like a calculator or vault.





HIDDEN APPLICATIONS

Password-Protected Apps — Vault, KeepSafe, and Best Secret Folder

Disguised Apps — Have you ever seen an app on your child's phone and wondered "What does that do?" Maybe an app that advertises volume or brightness control, when these controls are right on your child's phone?

Out of Place Folders — Title a folder "Health" or "Homework" It may sound too obvious to be true, but some teens create misleading folder names to help hide apps they know mom and dad won't like.











Crimes and Offenses

Cyberbullying (What is the law?)

- Makes cyber harassment illegal of a child (less than 18yrs of age)
- Includes the use of electronic communications directly through the child or the use of
- Social media service
- Requires a continuing course of conduct (pattern)
- Requires the intent to harass, annoy, or alarm a person
- Includes making disparaging statements or opinions about the child's: physical
- Characteristics, sexuality, sexual activity, mental or physical health
- Includes threats to inflict harm



LEGAL RESPONSE

- Cyber Harassment of a Child is a third degree Misdemeanor punishable up to one year of prison and/or \$1,000 fine.
- Juveniles that engage in Cyber Harassment the District Attorney's office has a diversion program for this crime.



CYBER BULLYING CASE CASES:

Student intentionally photoshopped a teacher's face and a student's face displayed in a pornographic position which was electronically transmitted to others in the high school. Student was identified and arrested for Cyber Harassment.

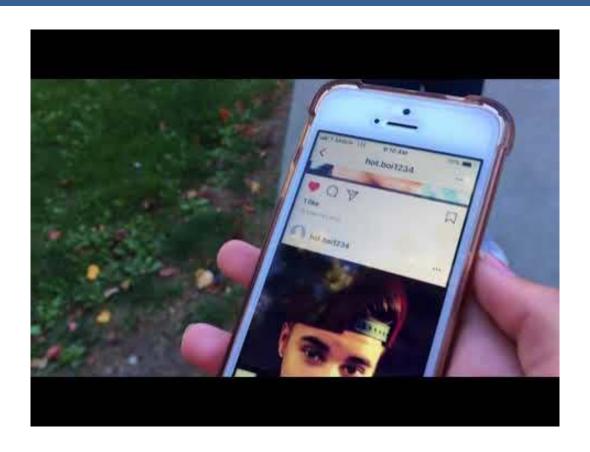
Student created a fictitious webpage mocking the victim who was a student at the high school. The webpage was made known to others including the victim. The victim printed out all the pages of the website and was able to identify the creator also another student. The student who created the webpage was arrested for Cyber Harassment.



WHO IS REALLY BEHIND THE PROFILE???









CATPHISHING

- Refers to setting up a fictitious profile with false information for the purpose of luring a minor.
- Fake photos or names are often used under false pretenses.
- Often times used for sexual advances or extracting money.



ONLINE ENTICEMENT CASE

- USER WOULD SEND OUT FICTITIOUS PROFILE PHOTOS OF A TEEN-AGE GIRL
- "CUTE STACEY" USED SEVERAL SOCIAL MEDIA APPLICATIONS TO MEET TEEN-AGED VICTIMS
- CONVINCED SEVERAL TEEN-AGED GIRLS TO SEND NUDE PHOTOS OF THEMSELVES
- AFTER POLICE INVESTIGATED AND FOUND THAT "CUTE STACEY" WAS ACTUALLY A 35YR OLD MAN





Sexting

- Knowing transmits, distributes, publishes, or disseminates an electronic communication containing a sexually explicit image of themselves.
- Knowing possesses/views a sexually explicit image of a minor 12 years old or older.
- Crime is a summary offense child will go through a diversion program.
- Example: Jen (15) sends a sexually explicit photo from her smartphone to Ryan (15) in which he possesses it.



Sexting Part II

- Knowing transmits, distributes, publishes, or disseminates an electronic communication containing a sexually explicit image of ANOTHER minor 12 years old or older.
- Crime is a Misdemeanor 3rd degree case referred to Juvenile Court
- Example: Greg (15) receives a sexually explicit picture from his girlfriend Shelby (15) and Greg sends that picture to his other minor aged friends.



Sexting Part III

- A minor with intent to coerce, intimidate, torture, harass, or cause emotional distress to another minor (a) takes a picture of minor without their consent or knowledge & (b) transmits such picture for a commercial purpose.
- Crime is a Misdemeanor 2nd degree referred to Juvenile Court
- Example: Rachael (16) snaps a photo of Megan (15) without her knowledge and threatens to show it to others unless she does homework for her. Brian (15) threatens to post a photo of Mary (15) on a social media website unless Mary does a favor for him.



SEXTING VIDEO





What can you do to protect and educate your child on proper use of social media?

- Educate yourself
- Understand that this is the world they live in
- Commonsensemedia.org Great resource to learn about new apps, movies, tv shows, etc. and if they
 are age appropriate
- Set guidelines and rules for how and when social media and online activity in general is permitted
- Talk to your children about the potential dangers online
- Keep the computer in a common area of the house
- Check your child's privacy settings on their device to ensure they are not allowing the general public access to their profile and personal information
- Use a shared Apple ID



Can I track my child's activity on their device?

- There are several apps that allow parents to maintain control over their child's device through an app
 - TeenSafe is one of the top rated apps
 - NetNanny
 - SecureTeen
 - RedPanicButton One touch button to instantly send your geographic location to your list of emergency contacts
- These should not be a replacement for open conversation and tough talks. They will always find another way to get to the content they want.
- iPhone built in GPS location services
 - Can show you where your family members geographical location is at any time





- 1. Report the incident to a parent. If occurs on-campus report to a principal and/or occurs off campus contact a law enforcement agency.
- 2. Do not retaliate back to the sender and stay off line is recommended.
- 3. Contact the social network (ex; Facebook) and file a report with them to aide the investigation.
- 4. Save all inappropriate content and/or take a screenshot of the violation.
- 5. Take steps to block the sender to deter future violations.

6. If the phone is under investigation - turn on "airplane mode" in order to prevent any remote deletion of important data.

