



Guide to
Social Media
in
**Educational
Environments**

In partnership with Social Sentinel, Inc.



Social Sentinel[®]

Assess. Alert. Avert.[®]

Table of Contents

Introduction	1
Social Media Defined	2
Mainstream Social Media Services	3
Social Media Challenges	5
Social Media Threat Alert Services	6
Uses of Social Media in Education	8
Summary	11

The National Center for Campus Public Safety Guide to Social Media was produced in partnership with Social Sentinel, Inc.
No federal grant funds were used in the production of this guidebook.

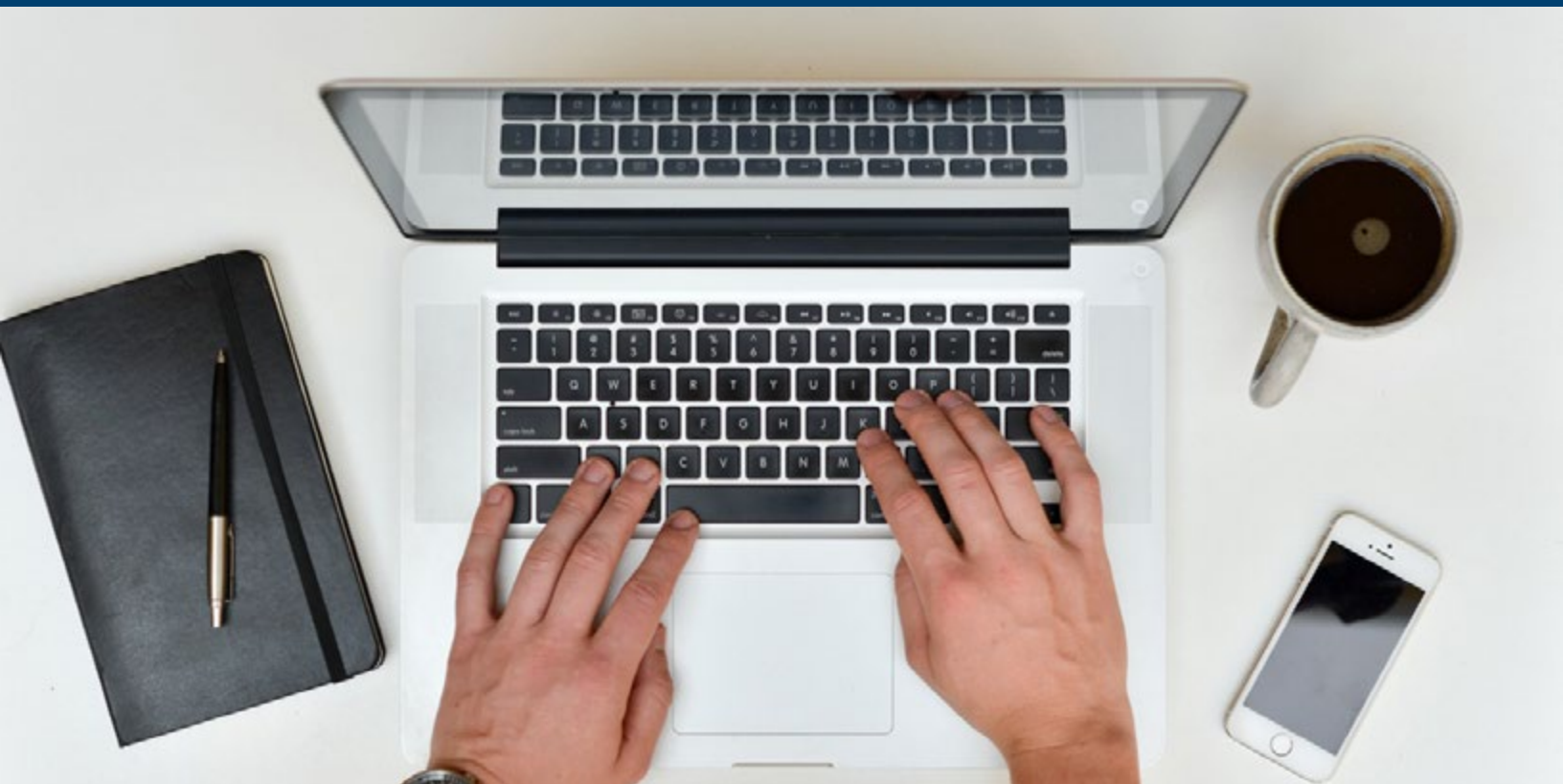
Introduction

Being responsible for the safety and security of a school district, college, or university is a unique challenge. The education culture fosters accessible environments that promote open sharing and community. Today's education leaders can no longer rely on their classroom experiences as the primary source of their effectiveness. They are facing a proliferation of technology that impacts almost every aspect of the learning environment. In particular, the technology of social media is changing how we communicate, and subsequently, how we learn.

The explosive growth of social media allows the unprecedented ability to instantly share every aspect of our lives. It is replacing the bulletin board and email, and fundamentally changing how we use a telephone. For many of the same reasons that schools use playground monitors and universities and colleges employ residence hall staff, it is becoming imperative that those responsible for the safety and security of our educational communities find respectful and efficient ways to engage the publicly available digital conversation.

This guide is brought to you by the [National Center for Campus Public Safety \(NCCPS at www.nccpsafety.org\)](http://www.nccpsafety.org), in partnership with [Social Sentinel, Inc. \(www.socialsentinel.com\)](http://www.socialsentinel.com). The NCCPS was established by Congress in 2013 to help fill a void in the campus safety community by providing a central repository of safety and security information and resources, and technical assistance and training to assist institutions of higher education in their efforts to enhance campus security and readiness. Led by Vermont-based [Margolis Healy \(www.margolishealy.com\)](http://www.margolishealy.com), a national consulting firm specializing in campus safety, security and regulatory compliance for higher education and K-12, the NCCPS is fulfilling its mission to support safer campus communities. [Social Sentinel, Inc.](http://www.socialsentinel.com) is a safety and security technology company, led and advised by respected safety officers and advocates. The company's flagship offering, the Social Sentinel® social media threat alert service, helps public safety officials better protect their respective communities by flagging potential threats shared publicly on social media sites.

The challenge for many is understanding what social media is and how it impacts safety in an educational setting. This guide intends to help those interested in the safety and security of a school district, college, or university with insight into the use and impact of social media.



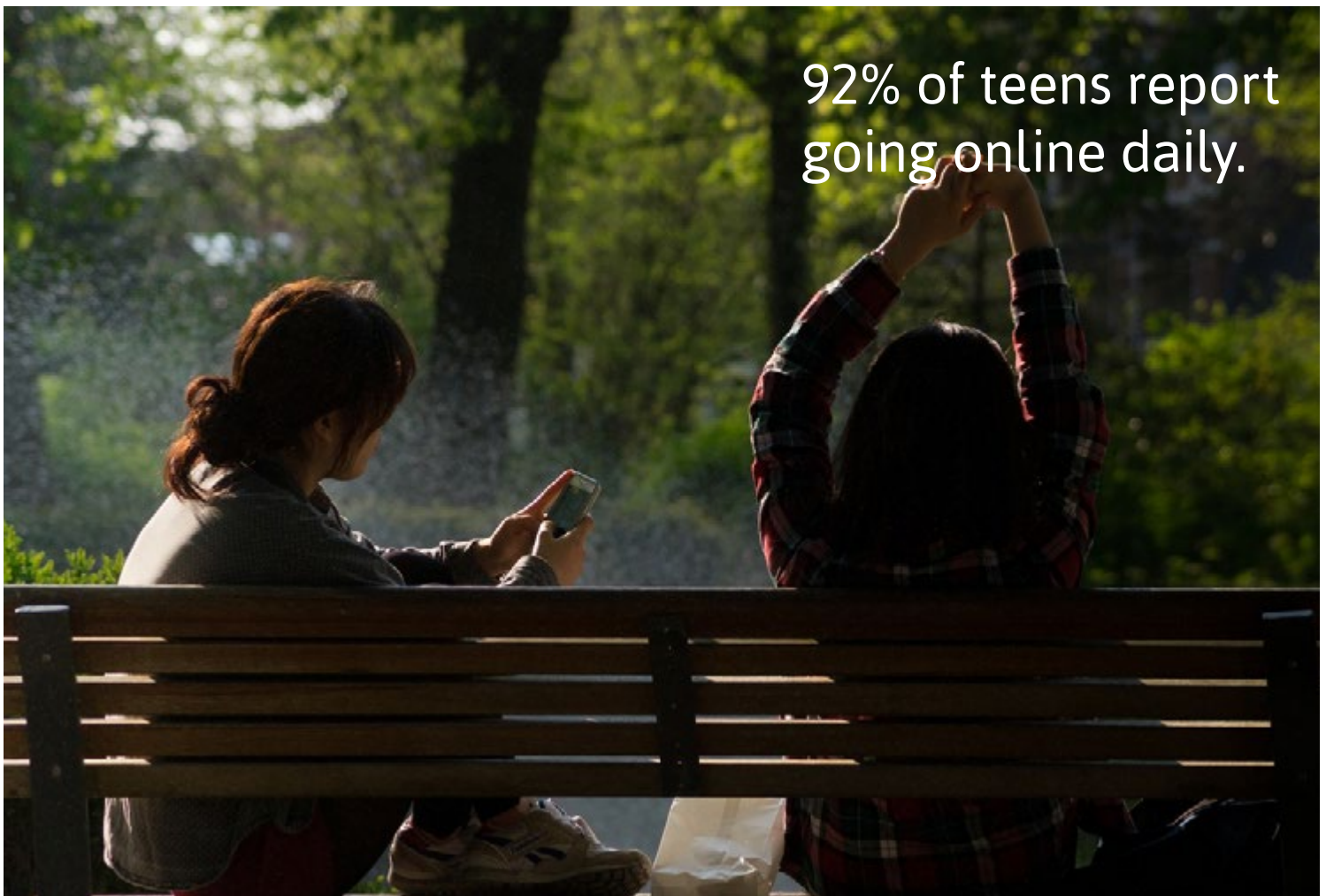
Social Media Defined

Social media is defined as websites or other applications (apps) that enable users to create, share, and view content or to participate in social networking by developing personal or professional networks. When it first appeared, the services were text based (e.g., Facebook, Twitter, electronic bulletin boards, RSS feeds, etc). It has evolved to images and short videos with the popularity of services like Instagram and SnapChat, and then to live video streaming with services like Periscope and Meerkat.

The use of social media by teenagers is no longer widespread—it is pervasive. Almost every middle school, high school, and college-age student in the United States engages in some form of social media. According to the Pew Research Center and consumer insight service Experian Simmons, 92% of teens report going online daily and 24% of teens are online “almost constantly.” This highlights the fact that mobile devices are commonly used in academic environments.

The 2015 CNN study, *#Being13: Inside the Secret World of Teens*, found that more than one third of eighth graders included in this study check social media without posting new information 25 times or more per day on weekends. Additionally, those who use social media the most admitted to checking their feeds more than 100 times a day, sometimes even during school hours. Child development experts examined the content of what 200 teens actually say and do on social media, and explored what it means to them. What they learned is insightful into the impact of social media on the lives of students. Some teens spend vast amounts of time online where they read the feeds of their peers’ activities and post things they’d never say in person.

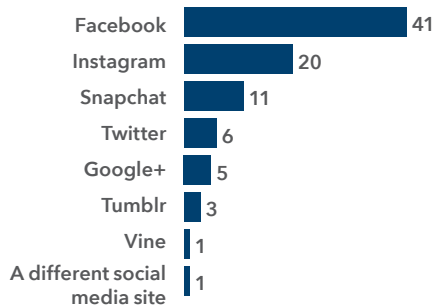
Mainstream social media services are constantly evolving. As of the publication of this guide, the following section describes the most popular services and their general uses.



Mainstream Social Media Services

Facebook, Instagram and Snapchat Used Most Often by American Teens


% of all teens who use _____ most often





Note: "Don't use any" responses not shown.


Source: Pew Research Center's Teens Relationships Survey, Sept. 25-Oct. 9, 2014 and Feb. 10-Mar. 18, 2015 (n=1,060 teens ages 13 to 17)


PEW RESEARCH CENTER


 **Facebook:** Originally designed for college students, this platform allows users to share information including pictures, videos, location, and their Facebook "friends." Privacy settings include blocking another user from seeing posts, whether or not that user is a friend. Facebook is the largest social media service in the world and remains a dominant social network for teens.

 **Instagram:** Owned by Facebook, users post photos and videos, and can easily share them across other social media platforms. Hashtag use, such as #yolo and #throwbackthursday, tags photos or videos and links it to other content or events. This makes it possible to search for and find content created by other users.


 **Snapchat:** Photos and videos can be shared with friends as "snaps" that are viewable for up to ten seconds or "stories" that may be viewed for 24 hours, after which they are no longer viewable. However, those viewing the content may take screenshots to store and share further. Users create their own friends list, and only receive snaps from those listed. Content can be enhanced with text, doodles, and emojis.


 **Twitter:** Users send and follow posts that are limited to 140 characters. Like Instagram, hashtags make it easy to follow a subject no matter who is posting about it. Many view it as a source for news rather than conversation, getting real-time updates on events and topics of interest.


 **Google+:** Google + is a social network that builds off of a Google account and has various sections within the platform to connect with other users. Google "Hangout" supports video chats with up to ten users, and hashtags can be added to all content. The popularity of this platform is likely due to its integration with the video sharing site, YouTube, as well as the ability to edit and share photos.


 **Tumblr:** Owned by Yahoo! Inc., this microblogging and social media site allows users to create their own blog where they can post text, photos, music, videos, and links. Users can follow other bloggers, or search posts by keywords or hashtags. All boards are public, so many users post under a pseudonym.

Video-based Platforms


 **YouTube:** Teens tend to view other users' "channels" more than they create and share their own on this popular site. Keyword searches help users find content of interest.


 **Vine:** Owned by Twitter, Vine is a video-sharing app where one- to six-second videos can be created, liked, and commented on. Users can follow each other and content can only be shared with Twitter, unlike many other sites that allow sharing on multiple platforms.


 **Vimeo:** This is another video sharing site that allows users to upload content, choose with whom to share, and follow or subscribe to other users' content.

 **Periscope and Meerkat:** These are both relatively new live-stream video-sharing apps. Key differences include Periscope's ability to save footage for 24 hours after it has aired and permit viewers to comment. Meerkat, which is independent from the other companies, reaches out to Twitter users' followers to announce their live videos.


Anonymous Apps


 **Yik Yak:** Users do not create profiles or usernames but instead remain anonymous when posting through this app. For college and university users, messages (“Yaks”) are sorted by geographic location and only posts within a 1.5 to 10 mile radius appear. Yik Yak does not allow posting from middle and high school locations.


 **Whisper:** This app allows people to share their secrets anonymously. Anonymous handles identify each user’s messages (“whispers”), and allow users to comment on each other’s whispers, or to start private chats. Whisper uses geographic locations to notify users of posts created by others within a certain radius. Users can sort their feed by school, location, keywords, most recent, and most popular.

 **Ask.fm:** This question and answer site is purportedly most popular with 11 to 14 year olds, although their policy states users have to be at least 13 years old. Under a self-generated username, users post questions that others can answer. Ask.fm is linked to Facebook and Twitter, so posts can easily be shared across platforms.

Messaging Apps

 **Kik:** Users post under a self-generated username, and create their own network of friends to communicate with by sharing pictures, video, text or other content. Messages from people outside of a user’s network appear blurry. However, the OinkText app linked to Kik allows messaging with strangers who share their Kik usernames. Kik is linked to other social media platforms so users can easily share content and make connections with other friends.

 **WhatsApp:** Owned by Facebook, WhatsApp, like Kik, allows users to message each other across social media apps and without incurring charges from their mobile carriers. As of September 2015, Whatsapp boasts a user base of nearly 900 million, making it one of the most popular messaging apps in the world.


 **ooVoo:** Unlike FaceTime, this free video chat app allows multiple users to chat together. It has privacy settings that allow users to select who can find them on the app.



Social Media Challenges

While problems have arisen on every social media platform, some are more prone to these abuses than others given their ability for anonymity and privacy. Some examples of issues originating from social media include threats of mass violence on campuses or proposed violence toward specific individuals or groups; controversial posts with racist, homophobic, and misogynist content; and sharing content that is harassing, defaming, or otherwise harmful.

Posts about self-harm are easily located across social media platforms; a quick hashtag search can yield multiple posts. Many social media companies have policies that prohibit images or posts about self-harm, including glorifying cutting, suicide, anorexia, or bulimia, but efforts to effectively filter harmful content are insufficient.



Over 25% of middle and high school students report that they have been cyberbullied.

Cyberbullying, or the willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices, occurs on every social media platform, including mainstream and anonymous sites. According to the Cyberbullying Research Center, over one quarter of middle and high school students report that they have been cyberbullied. A recent study by researchers at Pennsylvania State University and University of South Florida, Tampa, reveals that 19% of college students say they have been cyberbullied. States have responded by enacting and strengthening existing anti-cyberbullying legislation. Many states have enacted or proposed laws that specifically mention cyberbullying, but only some mandate that schools intervene if the cyberbullying originates from off school property. For more information on cyberbullying, visit The Cyberbullying Research Center at www.cyberbullying.org.

According to the Centers for Disease Control and Prevention (CDC), suicide is the third leading cause of death among young people, and for every suicide there are at least 100 suicide attempts. Some of these acts of self-harm are linked to cyberbullying. High-profile cases such as 16 year-old Amber Cornwell, 12 year-old Rebecca Sedwick, and 16 year-old Jessica Laney have raised deeply troubling concerns about online behavior.

Social media impersonation is a challenge for teachers and administrators. In what is often described as a form of cyberbullying, the perpetrator sets up a social media account using someone else's name and photo, and then posts defamatory content. In one instance, two former high school students were charged with multiple crimes for setting up a Twitter account using the name and photo of one of their teachers. A handful of states have statutes making cyber impersonation a felony.

Social Media Threat Alert Services

Given the prevalence of its use, paying attention to social media is an important component for school and campus safety, yet it is time-consuming and difficult to capture and sort through all relevant information. The 2015 Margolis Healy *Campus Safety Survey* found that two thirds of universities and colleges recognize the need to pay attention to publicly available social media for the safety of their communities, but only one third of those do so in an automated way. In higher education, this is largely a manual process. The 2014 LexisNexis *Social Media Use in Law Enforcement* report revealed that while 67% of law enforcement officers acknowledge the importance of social media monitoring as a crime-fighting tool, it is, according to researchers at Wright State University in Ohio, a “tedious and inexact process.” Without formal methods for the analysis and interpretation of social media data for crime prevention, all available information is not captured, and that information is not collected or updated at regular intervals.

Social media threat alert services can help schools and campuses keep up with potential safety and security issues. These services can separate insignificant information from legitimate threats and other credible safety concerns. The ways in which these services capture and share information vary and not all are appropriate for schools and campuses. Social media threat alert services appropriate for schools and campuses should:

- Have a primary focus on safety and security.
- Be able to provide documentation of legal agreements with all of the social media sites included in their services. These agreements should allow the service provider to access and share the data.
- Have the ability to perform searches within and outside of a geofence (a virtual perimeter for an actual geographic area).
- Include a comprehensive, updated keyword library of safety and security focused terms that have already been refined.
- Allow the addition of specific words or phrases to the user’s keyword library that are unique to their community.
- Clarify administrative and oversight control options.

Policy and Procedure Considerations

Determine who will be authorized to access the data. To get the most from your service, decide who on your team should have access. Choose at least one backup or alternate to the main administrator and consider providing access to additional team members, as appropriate. Limiting access to only one member of your team may constrain the ability to assess alerts and see the entire picture.

Assign library topics and alerts to the most appropriate user(s). You should be able to assign specific threat alerts to specific people on your team or in the school or campus community. For instance, depression and self-harm topics could likely be received by mental health services, while violence related alerts might be received by security staff. Additionally, limit what information each group can access. Ensure your system allows you to decide what each specific user can see and do. Providing universal access to a service’s alerts and settings without oversight can lead to problems.

Utilize a tiered approach to roles and permissions that align with your organization’s administrative structure. Create accountability through the established administrative hierarchy by limiting access and use, and allowing supervisors the ability to audit use of the service. This can help ensure the service is being used appropriately and according to policy and practice.

Develop a process users should follow when an alert warrants further inquiry or action. In many instances, their actions might follow existing protocols in public safety or threat assessment. Otherwise, the process users follow should be outlined and tied into existing policies and procedures.



Develop a process users should follow when an alert warrants further inquiry or action.

Procedures to Consider when a Threat Alert is Received

Nothing replaces human experience in evaluating threat alerts. When a credible threat alert is received, an inquiry should be conducted according to established procedures. Schools and campuses have protocols that address a wide range of threats, alerts, and tips, and may require review or investigation before a decision is made on the appropriate action. For example, social media users don't always use their real names, so it can take time to identify the person behind the posted content. Determining whether the threat alert is credible and/or relevant is critical before taking mitigating action.

Once an alert or threat meets the criteria established in policy and procedure, public safety officials, guidance counselors, or a school resource officer might be contacted, especially when an individual student posts about self-harm; involvement with illegal activity; physical violence, or bullying. Law enforcement or public safety officials may be contacted with advanced notice of a potential fight, flash mob, mass demonstration, or other situation that might require their attention for public safety purposes.

Officials might follow individual social media accounts to check for escalating language, comments from others, and trends that might effect the safety of the school or surrounding community. This use is sometimes described as "taking the temperature" of your community rather than being called to action. It might help identify areas in which dangerous activity is occurring, groups who are considering some type of illicit and/or dangerous activity, or the potential for rivalries to become dangerous.

Uses of Social Media in Education

Schools, colleges and universities should consider developing a social media strategy for disseminating information to their community members. Provided by the Office of Community Oriented Policing Services and the Police Executive Research Forum, the report entitled, *Social Media and Tactical Considerations for Law Enforcement*, lists the following considerations for developing a strategy to share information over social media:

- **Do not be afraid to take calculated risks:** An oversensitivity to risk assessment can thwart efforts to launch a social media program. It is easy to identify possible problems that could result from using social media, but police leaders in Toronto found that in practice, many of those problems did not materialize. They recommend focusing on the potential rewards of using social media, and working to mitigate the risks.
- **Identify the right people to use social media:** Not everyone is a “natural” at writing clearly and showing sensitivity to political and social considerations. But training can help improve these skills for many people. The people who are best at using social media view it as a useful and integral part of their job, not as a time-consuming chore.
- **Basic tips to remember:** There are certain ideas that always apply to social media, starting with the fact that “the Internet is forever.” That is to say, once a statement has been posted online, it can be impossible to take it back. Even if you delete the statement, it may already have been captured or recorded in various ways. So social media users must be careful to say exactly what they mean. Police also must be sensitive to the privacy of others, and should always be respectful and patient.



Social media sites may be used to disseminate information during campus emergencies such as criminal incidents, natural disasters, or health-related crises. They can be utilized as part of the emergency notification process mandated by the Clery Act. The University of Buffalo study, *Factors impacting the adoption of social network sites for emergency notification purposes in universities*, states social media not only enables campus officials to instantly reach a large percentage of students to provide timely and accurate information during crisis situations, but sending messages through social networking channels also means students are more likely to comply with emergency notifications received.

An increasing number of campus public safety and law enforcement agencies are using social media sites to understand illicit activity occurring on campus. The International Association of Chiefs of Police produced the following guide, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*. This guide is designed to direct law enforcement personnel through the development of a social media policy by identifying elements that should be considered when drafting a policy, as well as issues to consider, including privacy, civil rights, and civil liberties protections. This resource can be used to modify and enhance existing policies to include social media information. Any campus safety or law enforcement department, regardless of size, may benefit from the guidance identified in this resource.

Social media is being used for prevention efforts and raising awareness on timely and critical safety issues such as sexual assault, underage and high risk drinking, and mental health. Specific prevention strategies being implemented by colleges and universities, including social media campaigns, are provided in the White House Task Force to Protect Students From Sexual Assault Not Alone resource, *Preventing Sexual Violence on College Campuses: Lessons from Research and Practice*. The Task Force also issued the report,

Establishing Prevention Programming: Strategic Planning for Campuses, that provides key points to consider when strategic planning for sexual violence prevention. Both resources can be accessed through the National Center for Campus Public Safety (NCCPS) website, www.nccpsafety.org.

See Something, Say Something Message



The Department of Homeland Security's national campaign, If You See Something, Say Something, raises public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law enforcement. A variety of public service announcements that can be shared with community members are available on the campaign's website (www.dhs.gov/see-something-say-something/).

Spreading the "see something, say something" message, and making it easier for people to report are vital components to school and campus safety. Communities should consider setting up an anonymous tip line, publicizing existing reporting methods, or creating a social media presence that enhances public safety.

Basic Guidelines You Can Share

The National Cyber Security Alliance's *Stay Safe Online* website (www.staysafeonline.org) provides the following safety tips:

Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.

Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.

Your online reputation can be a good thing: Recent research also found that recruiters respond to a strong, positive personal brand online. So show your smarts, thoughtfulness, and mastery of the environment.

Keep personal info personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

Know and manage your friends: Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. Use tools to manage the information you share with friends in different groups or even have multiple online pages. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life.

Be honest if you're uncomfortable: If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them respect those differences.

Know what action to take: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

See more at StaySafeOnline.org.

Advice from the FBI

The Federal Bureau of Investigation (FBI) educational material, *Internet Social Networking Risks*, provides the following specific risks to be aware of when using social media:



Baiting - Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer. Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

Click-jacking - Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social networking sites. Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

Cross-Site Scripting (XSS) - Malicious code is injected into a benign or trusted website. A Stored XSS Attack is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A Reflected XSS Attack is when a person is tricked into clicking on a malicious link; the injected code travels to the server then reflects the attack back to the victim's browser. The computer deems the code is from a "trusted" source. Turn off "HTTP TRACE" support on all web servers. Research additional ways to prevent becoming a victim of XSS.

Doxing - Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles. Be careful what information you share about yourself, family, and friends (online, in print, and in person).

Elicitation - The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. Be aware of elicitation tactics and the way social engineers try to obtain personal information.

Pharming - Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. (E.g.: mimicking bank websites.) Watch out for website URLs that use variations in spelling or domain names, or use ".com" instead of ".gov", for example. Type a website's address rather than clicking on a link.

Phishing - Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim. Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it.

Summary

Today's social media services have evolved far beyond their beginnings, and are creating previously unimagined opportunities for human expression while at the same time creating challenges for our individual and collective safety. This guide is intended as a primer for participating in the digital conversation. By contributing to the conversation through social media, we are able to communicate critical and important information relevant to the safety and security of our school campus communities. By listening respectfully to the digital conversation, we are able to identify potential threats against safety and take action to prevent potential tragedies.



Sources used:

<https://www.socialsentinel.com/>

<http://www.margolishealy.com/>

http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf

<http://www.adweek.com/socialtimes/teens-millennials-twitter-facebook-youtube/496770>

<http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/>

<http://www.emarketer.com/Article/Teens-Press-Play-on-YouTube/1010629>

<https://www.common sense media.org/blog/15-apps-and-websites-kids-are-heading-to-after-facebook>

<http://www.theatlantic.com/technology/archive/2015/04/whats-stopping-people-from-periscoping-copyrighted-material/389228/>

<http://www.businessinsider.com/the-inside-story-of-yik-yak-2015-3>

<http://nymag.com/daily/intelligencer/2014/06/complete-guide-to-anonymous-apps.html>

<http://cyberbullying.org/summary-of-our-research-2/>

<http://www.usnews.com/news/articles/2015/05/29/is-social-media-making-self-harm-worse-for-teens>

<http://www.emergencymgmt.com/disaster/Social-Media-Communication-Campus-Emergencies.html>

<http://www.nccpsafety.org/resources/library/social-media-and-tactical-considerations-for-law-enforcement/>

<http://www.nccpsafety.org/resources/library/establishing-prevention-programming-strategic-planning-for-campuses/>

<https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks>

<https://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>

<http://www.cnn.com/2015/10/05/opinions/underwood-faris-being-thirteen-lurking-social-media/index.html>