



The State University
of New York

DRAFT REPORT OF THE CHANCELLOR'S TASK FORCE ON SOCIAL MEDIA RESPONSIBILITY

Submitted to the SUNY Board of Trustees
September 10, 2015

CO-CHAIRS

Rachel Haot, Chief Digital Officer and Deputy Secretary for Technology

Zvi Szafran, President, SUNY Canton



Draft Report of the Chancellor's Task Force on Social Media Responsibility

I. Introduction

As social media transforms society, its impact on higher education institutions raises significant questions on how schools can successfully keep pace while supporting a safe and healthy campus environment.

Propelled by expanded broadband Internet access, accessible creative technologies, powerful mobile devices and the first digitally native generation, universities exist at the nexus of dynamic developments that are redefining the college experience.

For the digitally native generation, learning and socializing--two core elements of campus life--take place both online and off. As a result, young adults are expressing themselves on new digital platforms, with benefits and consequences that challenge the existing systems. What's more, the nature of these platforms change on a daily basis, as young adults aware of the web's permanent record flock to apps centered on anonymity and ephemerality, where they may feel they can interact more freely.

Collectively, these changes demand a new policy framework that supports the evolving nature of campus life. Reflecting this need, in February, 2015 SUNY Chancellor Nancy Zimpher convened a task force to analyze the impact of social media and provide recommendations on educating the campus community and responding to safety challenges.

Composed of faculty, student, law enforcement and government representatives, the task force studied past incidents, consulted with industry experts and developed a set of flexible recommendations to support SUNY institutions as they modernize policy and programs in the digital age.

This report details the charge by Chancellor Zimpher, the rise of social media, a social media-enabled incident at SUNY Canton involving anonymous platform Yik Yak, and the makeup of the task force itself. It concludes with a set of eight flexible recommendations related to policy principles, digital citizenship, incorporation into existing codes of conduct, community awareness and education, reporting protocols, and emergency preparedness and communication.

As technology transforms higher education and campus life, the Chancellor's Task Force on Social Media Responsibility reflects SUNY's commitment to supporting safe, healthy, constructive communities that embrace change and uphold institutional values both onscreen and off.

II. Charge

Incidents related to anonymous social networks such as Yik Yak have been making the headlines as schools and campuses see an increase of occurrences.

In light of recent experiences at several SUNY campuses, Chancellor Zimpher decided to establish a Task Force on Social Media Responsibility.

The charge to the Task Force was to develop system-wide recommendations to be presented publicly to SUNY's Board of Trustees, and shared with national higher education organizations to help assist other universities across the country in tackling issues related to social media responsibility.

The Task Force, consisting of experts in the field, was to consider strategies for improving social media responsibility on campuses, with two overarching principles:

1) **Education:** Students need to understand the consequences of using social media platforms and the responsibility, respect, and judgment that they should exercise in both anonymous and identified settings. These efforts might include topics such as protecting one's online reputation, understanding the damage of cyber bullying, and understanding the consequences of making online threats.

2) **Response:** When a threat occurs, University Police and campus administrators need to know how to respond. Guidance and best practices around communication, protocol, decision making, investigation, and potential changes to the student code of conduct can take much of the guesswork out of an already stressful situation.

III. Background

The history of social media began in 1991 with the advent of the World Wide Web, created by Tim Berners-Lee, based on egalitarian principles to promote communication and sharing among users. The proliferation of Internet applications and platforms, termed *social media*, began just after the turn of the century and has evolved in sophistication and magnitude since that time. Facebook indicates that 1.39 billion people are currently members, a number slightly larger than the estimated population of China. Social media can be best described as a group of Internet-based applications that advance the ideological and technological substrate of next generation Web capabilities, and that support the digital creation and exchange of user-generated content.

The only thing uniform about social media is the complete differences between platforms. Some platforms such as Facebook and LinkedIn require identification of the user with their actual identity while others allow pseudonymous membership, including Twitter, Myspace, the Tumblr. Still others are completely anonymous where the identity is masked or inapplicable, such as Yik Yak. Still others like Snapchat delete content and keep it private by default. Students use these platforms for very different purposes, and the ink will not be long dry on this document before new platforms and methods bubble up.

Within the State University of New York system, the first major Yik Yak incident occurred at SUNY Canton, located in St. Lawrence County, 18 miles from the Canadian border. A post was discovered in the middle of the evening on October 22, 2014 indicating that a student was planning to take their own life and the lives of others on campus as well. **[See Appendix A]**

On November 4, 2014, a threat against another SUNY campus was posted on Yik Yak, threatening to blow up the University at Albany. The posting was signed with a false Arabic name. Following FBI guidelines, the University Police determined that the threat did not have a high degree of credibility. The University Police contacted Yik Yak. With information from them as well as support from the university's IT staff, the University Police were able to trace the post to an 18-year-old student. A search of his room did not turn up any bomb making supplies. The student faced a felony charge of falsely reporting an incident.^{1 2}

¹ Liz Holliday, "Police make arrest in UAlbany bomb threat posted to Yik Yak", News10.com, November 6, 2014; <http://news10.com/2014/11/06/police-make-arrest-in-ualbany-bomb-threat-posted-to-yik-yak/>

² Kassie Parisi, "UAlbany student is arrested after making bomb threat on Yik Yak", Albany Student Press, November 6, 2014; <http://www.albanystudentpress.net/ualbany-student-is-arrested-after-making-bomb-threat-on-yik-yak/>

As a result of these and other incidents, a debate ensued across the nation about how to deal with anonymous social media sites. Among the highest concerns was that such apps were becoming popular with younger children, in middle schools and high schools. Yik Yak engaged Maponics, a company that “builds and defines geographic boundaries” to map elementary, middle and high schools around the country to effectively keep the app from being used on their properties. The “geo-fence” strategy is now in place for the large majority of these schools³. Several college campuses banned the use of Yik Yak and other “anonymous” social media sites, and articles have appeared calling on other campuses to join the ban⁴, or arguing that it would be counterproductive to do so⁵.

Similar debates took place within SUNY. A system-wide notification was sent by Chancellor Zimpher to the SUNY presidents, alerting them to the incident that had taken place at SUNY Canton. The Chancellor noted:

“What makes this incident different from others we may have seen or encountered in the past is the medium through which the threats were made. Anonymous social networks like Yik Yak present a new kind of challenge in keeping our campuses safe. There is a delicate balance we must work to find in keeping our institutions functional in the face of irresponsible and unaccountable digital threats, while at the same time placing the safety of our students and the campus community as our highest priority.”

Chancellor Zimpher called on each campus to inform the system as to what approach they had taken in addressing these types of concerns. This led to conversations throughout the SUNY system. At Oswego State, for example, President Deborah Stanley held a meeting reviewing campus emergency responses, and discussed the possibility of banning Yik Yak. It was ultimately decided that banning Yik Yak would be an infringement of freedom of speech, and that it would also be futile—another app would replace it⁶.

IV. Process

In December 2014, Chancellor Zimpher announced the establishment of a Task Force on Social Media Responsibility, asking SUNY Canton’s President Szafran and New York State’s Chief Digital Officer, Rachel Haot, to serve as co-chairs, assisted by David Belsky, SUNY’s Director of Marketing & Creative Services. The charge to the task force would be “to develop system-wide recommendations around education to prevent social media abuse, as well as guidance on how to respond when a threat does occur.

After some discussion, the membership of the committee was determined, consisting of representatives from faculty, counsel, law enforcement, technology, communications, student affairs, campus leadership, system leadership, and students:

Name	Organization	Title	Role
Rachel Haot	Executive Chamber	Chief Digital Officer	Co-Chair
Zvi Szafran	SUNY Canton	President	Co-Chair
Reynol Junco	Harvard University	Associate Professor & Fellow	Academic Expert
Joseph Storch	SUNY System	Associate Counsel	Counsel

³ Diana Graber, “Yik Yak App Makers Do the Right Thing”, Huffington Post, March 26, 2014; http://www.huffingtonpost.com/diana-graber/yik-yak-app-makers-do-the_b_5029679.html

⁴ Ryan Chapin Mach, “Why Your College Campus Should Ban Yik Yak”, Huffington Post, December 3, 2014. http://www.huffingtonpost.com/ryan-chapin-mach/why-your-college-campus-should-ban-yik-yak_b_5924352.html

⁵ Larry Magid, “Banning Yik Yak from College Campuses is Counterproductive”, Huffington Post, January 3, 2015. http://www.huffingtonpost.com/larry-magid/banning-yik-yak-from-coll_b_6779168.html

⁶ JoAnn DeLauter, “Yik Yak raises campus safety concerns”, The Oswegonian, November 6, 2014; <http://www.oswegonian.com/2014/11/06/yik-yak-raises-campus-safety-concerns/>

Paul Berger	SUNY System	SUNY Police Commissioner	Law Enforcement
Bruce McBride	SUNY System	SUNY Police Commissioner, Ret.	Law Enforcement
Sam Conn	SUNY Empire State	Chief Information Officer	Technology
Ryan Yarosh	Binghamton University	Director of Media & Public Relations	Communications
Scott Titus	Onondaga Community College	Director of Marketing & New Media	Student Affairs
Martha Asselin	Schenectady County Community College	Acting President	Campus Leadership
Jennifer LoTurco	SUNY System	Assoc. Vice Chancellor for External Affairs	System Leadership
James Corra	Student Assembly (State-Operated)	Director of Communications	State-Op Student
Christopher Wallace	Student Assembly (Community College)	Deputy Director of New Media	CC Student
Rosalyn Rufer	University Faculty Senate	Member	State-Op Faculty
Leanne Warshauer	Faculty Council of Community Colleges	Press Officer	CC Faculty
Jerald Jones Woolfolk	SUNY Oswego	Vice President for Student Affairs and Enrollment Management	Campus Leadership

The Task Force met for the first time on June 18, 2015 in Albany, NY. Subsequent meetings were held on July 6, 2015 in New York City, and July 23, 2015 in Albany. The July 23 meeting resulted in a report to the SUNY Board of Regents being outlined. Volunteers were taken to draft each outline topic, with an overall draft to be produced by Belsky, Haot, and Szafran to be shared with the Task Force.

V. Recommendations

A. General

i. Social Media is Powerful, and Responsible Use Can Have Positive Impact

The Internet and World Wide Web are inherently neutral, meaning that the technology is not good or bad in a societal context. Social media applications and platforms that reside on the Web reflect society much like other public forums, but often in a *magnified sense* because of worldwide reach and ease of access and use. Social media comes in many forms, from information repositories like Wikipedia, to conversational and visual forums such as Facebook, YouTube, Pinterest, Twitter, and LinkedIn. Almost too numerous to count, new social media applications and platforms are released each day. Social media has altered the nature of public and private communication, and has provided benefit to people worldwide through its ability to facilitate community, discovery, sharing, and learning.

While irresponsible uses of social media draw the majority of news coverage, social media has been used to find runaway children and keep them connected to their families, support people during difficult times, change how elected officials interact with constituents, fund worthy charities and projects, build a more collaborative workforce, spread religious belief, and promote health. One of the most positive things about social media is that it has democratized the World Wide Web. Anyone can create, interact, engage, and provide opinions via platforms that enable uploading of content items, discussions, and public forums. The ability to crowdsource data (gather contributions from a large group of people) has demonstrated amazing predictive capabilities, drawing accurate results from the general public. Social activities such as talking with friends, exchanging stories, sharing pictures, checking-in with others, and “liking” things are possible at any time and in any place. The nascent use of social media in education has

been widely funded and is of interest to scholars worldwide; the potential for new education-based social media platforms has yet to realize full potential. In sum, social media possesses huge potential for societal good if digital citizenry use these capabilities in a responsible manner.

Recommendation 1: Universities should treat social media primarily as a positive tool and not try to restrict its use.

ii. Digital vs. In-Person: What's the difference?

The most notable differences between the digital (i.e., virtual) world and the in-person physical world involve *wider* distribution of *immediate* content, wider *public access* to the content, and in most cases a *permanent record* of events and communications. Social media can be an important tool in building the type of world we want to live in. For social media to reach its potential of supporting such worthy goals such as friendship, learning, cross-culturalization, sharing of information, and communication, digital citizenship should be grounded in emotional intelligence, healthy boundaries, and proper societal governance.

Recent generations more easily blur the lines between the virtual and physical worlds. Examples include a predisposition to text rather than call, to post “selfies”, to blog opinions, and to post near real-time videos. More photographs are being taken, more videos are being produced, and more opinions are being shared than at any time in history. As a result, responsible digital citizenship has become an important societal element as we move into the 21st Century.

Societal norms should transcend to the virtual world, but in some instances fail to do so. The way some people act online is often an exaggerated form of what they do face-to-face. They may use harsher language; make accusations or assumptions based on little or no evidence; share photographs that are more extreme; act in ways that are racist or sexist; and promote one-sided political views, calling those who disagree traitors or worse. Others online then feel a need to respond with equal or greater venom. Pretty soon, the interaction degenerates into a sequence of insults and threats.

Responsible digital citizenship requires the understanding that digital activity, particularly with regard to social media, leaves a lasting “footprint.” Such digital footprints can follow an individual throughout his or her lifetime and consequentially impact future opportunities. One’s digital identity is amplified through the Internet via its worldwide reach, accessibility to information, and lack of privacy. Digital activities accumulate with time, creating a lasting footprint that is easily found using conventional search engines. Social media plays a large role in setting one’s digital footprint, and to that end responsible and accountable behaviors are important. Mistakenly, many people believe the “veil of the Internet” provides anonymity and protection, and thus may lead to atypical or even reckless behaviors. Much like the physical world, the virtual world of social media can fall prey to bad actors and those who may seek to do others harm.

In addition, most theoretically “anonymous” applications are linked to real-world individual identities, and most companies will reveal personal information to the authorities if presented with a legal subpoena or warrant. Students and faculty alike should be aware that any illegal digital activity—whether anonymous or not—carries real-world consequences and can be easily prosecuted.

Recommendation 2: Digital citizenship is a necessary element in any contemporary university curriculum. Students should learn that social media can be an important tool in building a supportive community and that a permanent, public digital footprint is created from their participation.

B. Education

As a university system, SUNY's primary response to social media issues should be educational. What is the best way to create campus policies in this area? How can we educate our students, faculty, and staff to encourage responsible behavior and support positive use of social media?

i. Setting a Social Media Policy

Given the ubiquitous nature of social media, the Task Force concluded that every university should have a social media policy, but not necessarily a *stand alone* policy.

Almost every campus has an existing code of student social behavior that has been developed in a transparent and consultative fashion involving multiple stakeholders, often with significant student input. Similarly, at most campuses, students play a significant role in the campus' formal conduct process—participating on committees that hear cases and appeals, and helping decide what penalties to set. These existing codes can become the basis for an updated policy that incorporates social media behavior.⁷

Many online offenses have direct parallels to face to face offenses. In these cases, there is no reason to treat the two differently, and the social media aspect can be added directly. For example, a student posting a threat to harm a specific individual on a social media site should be treated the same as one who makes an analog written or verbal threat. A student engaging in online hazing of another student should be treated the same as one who physically hazed another student. While threats or racist comments on anonymous social media sites may pose distinct challenges in identifying the perpetrators, so do anonymous threats or racist graffiti written on rest room walls. Similar investigative procedures should be followed, with similar outcomes.

Effective codes of student behavior are much more than lists of prohibited activities. They paint a picture of an inclusive and engaging campus environment. They often include a discussion of the values that help create a unique campus identity. In a similar manner, social media values that parallel these campus values should be incorporated into these discussions and documents.

Recommendation 3: Each university should incorporate social media policy into its existing campus social policies and student codes of conduct, following the same consultative and transparent procedures that developed the earlier policies.

ii. Reporting Information

"If You See Something, Say Something" is a globally recognized campaign that was born in the wake of 9/11 as a tactic to involve citizens in efforts to prevent acts of terrorism. One of the main goals of this campaign is to encourage people to think of preserving not only their own safety, but also to take actions to preserve the safety of their community. The concept of not being passive when you see something that could be harmful to others can be applied to social media as well.

It is impossible for SUNY institutions to monitor all social media activity taking place at or referencing their school. They must rely on their communities to help, by encouraging them to pro-actively alert the institution to issues of concern they see on social media. An obvious example would be reporting a threat to life posted on social media (such as occurred at SUNY Canton). Other situations include reporting cyberbullying, self-harm, illegal behavior, or other similar serious negative events that can be prevented if responsible individuals are alerted.

⁷ Junco, R. (2011). The need for student social media policies. *Educause Review*, 46(1), 60-61.

Recommendation 4: All campuses should develop and communicate a process for community members to report concerns regarding social media content so that it can be assessed and addressed by the institution.

iii. Maintaining a Digital Identity

1. As a student

Students should understand that their interactions with others on social media should have the same attributes as interactions in person. Character, values and integrity should not change based on setting. Whether they are in the classroom, in the residence halls, or on social media, students should use the same judgment and exhibit the same values in how they interact with other people.

The goal is to create a social media community where every person feels respected and where people act in ways that do not impair their futures or cause harm to others. By maintaining professional, responsible digital identities, students can proactively improve the social media community and establish their own successful online reputation.

It is prudent to be thoughtful when deciding what to post online. Students should treat every aspect of their social media profiles as if a potential employer might scrutinize the details of their accounts at any time. Student social media accounts should avoid mention of illegal or unprofessional activities. Their presence can lead to an employer's decision not to hire a candidate.

Threats conveyed over social media have real legal consequences, even if made in jest and/or via theoretically anonymous applications. Many students are unaware that others who have made threats online, including threats that were believed to be anonymous, may face significant prison time as a consequence for their actions. Threats made online, even when analyzed not to be serious, are not taken lightly and should not be posted under any circumstances.

2. As a faculty member

Faculty create digital identities in two common ways: first, as an educator interacting with students and second, as individuals with their own personal social presence. As members of the SUNY community, faculty members are not immune from the benefits or the responsibilities that come with having a digital footprint.

Effective educators recognize the role that social media can play in the classroom. For the millennial generation, social media can be used to build engagement. Many papers and articles have been written about how to use social media in the classroom and the role that faculty should assume if they decide to use it as part of their pedagogy.^{8,9} Best practices that have been learned in other digital platforms should be followed, including those that highlight our best work and create welcoming learning environments for our students.

Faculty members should recognize that unlike online learning platforms that are designed and implemented with enhanced security by the university, social media platforms do not have the same levels of security and thus must be used with caution to ensure compliance with Family Educational Rights & Privacy Act (FERPA) regulations. For example, grades or student evaluations must never be

⁸ Vicki Davis, "A Guidebook for Social Media in the Classroom", February 19, 2015, <http://www.edutopia.org/blog/guidebook-social-media-in-classroom-vicki-davis>

⁹ Eric Klopfer, Scot Osterweil, Jennifer Groff, Jason Haas, "Using the Technology of Today in the Classroom Today: The Instructional Power of Digital Games, Social Networking, Simulations and How Teachers Can Leverage Them", http://education.mit.edu/wp-content/uploads/2015/01/GamesSimsSocNets_EdArcade.pdf

discussed or posted on a social media site. Faculty members must also ensure that online discussions take place in a welcoming and safe environment. The faculty member should actively monitor the discussion and have a de-escalation and resolution process that aligns with the terms of use of the social media platform.

In their own personal social media presence, while academic freedom allows for discourse from a variety of perspectives, this freedom does not extend to messages that are threatening to the SUNY community or its stakeholders, or that violate terms of employment. As faculty create their own social media presence, they should be aware that they are perceived as representatives of SUNY by the outside world, and that their posts are visible to students who may be “friends” or “followers”. Once a message has been posted to social media, it is almost impossible to retract. Just as we remind students that their digital identity will follow them long after their post, faculty too should pay attention to this message.

3. When representing a campus

Staff members representing their campus on social media should have clearly stated roles and goals agreed upon by campus leadership. The same level of responsibility should be implemented when engaging on social media as when issuing a news release or going on record with a reporter. The following best practices apply:

- If you participate in a social media site on behalf of the campus, discuss with your supervisor when you are empowered to respond directly to users and when you may need approval.
- If you have been authorized by your supervisor to create an official social media site or upload materials to one, contact the university’s Office of Communications and Marketing for approved logos and other images to ensure coordination with other sites and content.
- Be respectful. SUNY universities are committed to respect for the dignity of others and to the civil and thoughtful discussion of opposing ideas. Online communities can be volatile, tempting users to behave in ways they otherwise wouldn’t. Your campus’ reputation is best served when you remain above the fray.
- If you have any questions about whether it is appropriate to write about certain kinds of material, discuss it with your supervisor before you post.
- Be familiar with the terms of service and policies of sites and networks in which you participate. Pay attention to updates.
- Keep your personal views separate. Uphold the university’s mission and values in your posts.

iv. Developing an Educational Procedure

Education is a critical tool for SUNY institutions to maximize the positive use and minimize the negative use of social media on their campuses. This instruction needs to be grounded in positive examples. A literature review of Youth, Privacy and Reputation by the Berkman Center for Internet and Society at Harvard University indicates that by exaggerating risks and using scare tactics, a social media responsibility education campaign can actually have an opposite effect on how likely students are to engage in negative digital behavior.¹⁰

¹⁰ Marwick, Alice E. and Murgia-Diaz, Diego and Palfrey, John G., Youth, Privacy and Reputation (Literature Review). Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10-29. Available at SSRN: <http://ssrn.com/abstract=1588163>

Many campuses offer students first year orientation courses or programs that can serve as ideal locations to house a social media educational effort. The following topics might be included:

- What is social media?
- How does the campus use social media?
- Do you need a social media account?
- What are relevant policies for social media use by the campus community, and where can they be found?
- Best practices for a successful social media presence
- Cultivating your digital footprint
- Legal issues
- Social Media Do's and Don'ts

In addition to campus-based orientation courses or programs, the Task Force felt it would be desirable to develop a "Social Media and College" Massive Open Online Course (MOOC) for new student orientation and for employee training across SUNY. In conjunction with the MOOC, a system wide e-citizenship education campaign should be developed, focusing on positive examples and including a centralized communication toolkit with elements such as posters, handouts, digital banners, social media posts, videos, websites, etc. These resources would be available for any campus to use as they felt appropriate at their institutions.

Recommendation 5: Each university should provide instruction to students in an appropriate place in the curriculum (such as first-year orientation courses or programs) on how to maintain a professional digital identity. Students should be informed that all illegal activity, even if perpetuated on a theoretically anonymous or ephemeral platform, can be prosecuted and carry consequences.

Recommendation 6: Each university should provide training to faculty and relevant staff in appropriate use of social media. A system-wide MOOC on "Social Media and College" and an e-Citizenship campaign should be created for this purpose.

C. Response

The following material is not intended to be a comprehensive discussion of threat analysis or critical incident response on campus. Questions regarding these topics should be addressed to the University Police or community college Public Safety at each campus. It is a best practice for campuses to develop specific plans for this type of incident and to test the plans through regular tabletop, functional, or full-scale exercises.

i. Monitoring

While routine monitoring of social media platforms by institutions is not recommended due to resource, staffing, and liability concerns, social media can be a valuable communications tool during critical incidents, natural disasters, or special events. In these limited circumstances the campus media office would be the most appropriate venue for monitoring. It may also be useful to provide a single digital point of contact for students and faculty to report alarming activity, including automatic response with instructions on preserving the original digital content for analysis (e ii).

ii. Identifying a problem

It is most likely that the initial report of the threatening message will come from a community member and not from a campus official. Given the ephemeral nature of some social media platforms it is critically important that the message be preserved as soon as discovered. There are several relatively simple methods to preserving the message such as print, screen capture, or photographing the screen. Once

the message has been preserved law enforcement should be contacted. If the receiver is on campus, either the University Police or campus Public Safety should be called. If off campus, the local police agency or state troopers should be called. Once law enforcement has been contacted they will document the incident and begin the threat analysis process.

iii. Threat Analysis and incident response

Once the University Police or Public Safety has been notified of the threat they will begin the process of analyzing the threat. The factors used by law enforcement in threat analysis will not be specified in this document for security reasons. In addition to analyzing the threat, University Police or Public Safety will begin notifying campus leadership of the threat and their informed opinion on the validity of the threat. Other notifications may be made to SUNY System Administration and to local or other law enforcement agencies for technical or operational support if needed.

If the threat is determined to be non-credible, the University Police or Public Safety should initiate an investigation into the threat to determine if there was a violation of law in the message. Additionally, the University Police or Public Safety should consider limited monitoring of the social media platform the message was received on for additional messages or other information. Consideration should also be made to adopting a heightened patrol posture with additional personnel during the threat time frame so as to reassure any community members who also saw, or otherwise learned about the message.

If the threat is determined to be credible, the University Police or Public Safety should initiate a criminal investigation. The Chief of Police, Director of Public Safety and/or their designees will advise campus leadership on response options and suggested changes to campus status including limited/full evacuations, sheltering in place, building closures, and class cancellations. Monitoring of the social media platform that the threat was on should take place during the incident. The University Police or Public Safety should deploy personnel and other resources to counter the threatened action. There should be consideration of activating the campus emergency management plan to manage the personnel and resources, including the public information function. If significant amounts of outside resources are involved, a unified command structure may be most effective in managing the incident.

iv. Threat Preparedness and Education

Institutions of higher education will encounter various types of critical incidents (such as evacuation, missing student, threat of harm, violent act, natural disasters) and therefore, need to continuously update emergency response plans that reflect both proactive and preventive measures.^{11 12} Educational institutions have the duty to ensure a safe, healthy environment for all while addressing public policies making critical incident management a priority (U.S. Department of Education, 2009).

Lessons learned from critical incidents help to guide institutions of higher education in refining their campus emergency preparedness plans. Successful emergency plans have incorporated measures, policies and practices shared from the knowledge gained from past events experienced by similar organizations. These plans require innovative, coordinated, interoperable responses with overarching

¹¹ Duncan, M.A. and K.M. Miser. 2000. *Dealing with campus crisis*. In M.J. Barr, M.K. Desler, & Associates. 2000. *The handbook of student affairs administration*, 2nd ed. San Francisco; Jossey-Bass.

¹² Zdziarski II, E. 2006. *Crisis in the context of higher education*. In K. Haper, B. Paterson, & E. Zdziarski, II (Eds.). *Crisis management: Responding from the heart*. Washington, D.C.: National Association of Student Personnel Administrators (NASPA), 3-24.

strategies¹³ for the protection of lives and property, and the continuity or restoration of normal operations. Lessons learned from both actual incidents and exercises to test an institution's responses will help organizations prepare for future critical incidents.

The Clery Act (18 USC 1092(f)) does not mandate how institutions of higher education are to issue mandated timely notice of a critical incident; however, all campuses must demonstrate redundancy in tools for communicating "timely warnings" in the event of an emergency. Social networks should be considered as a platform for critical incident management and offer a vehicle for communicating in the event of an emergency. Good practices utilize social networks in a positive fashion as a means for informing and mobilizing others during a critical incident.

With that said, institutions of higher education must also consider the malicious potential and compounding effects of social networks when planning threat preparedness and training. Critical incident management planning must consider the reactionary, impulsive and spontaneous nature of interactions on social networks. When planning, manager should understand that social networks can be used to push forward harmful or misleading information, turn a low-key incident into a critical incident and have the potential to cause a secondary critical incident to develop (such as media response, parent concerns, copycats). Such considerations should be weighed when planning responses to social media threats.

Critical incident management plans should consider how to address the public relations damage that could result in negative consequence from inadequate communications during an incident. Immediate and accurate information released throughout all phases of the critical incident is in everyone's best interest. A good practice for institutions of higher education is to stay abreast of potential opportunities, challenges, threats and constraints when considering social networks.

Recommendation #7: Campuses should collaborate in developing a well prepared social media policy, code of conduct, and training program. In addition, campuses within the system should know what other campuses might be available to assist with monitoring social media activity in the aftermath of a campus critical incident.

v. Notification

Institutions of higher education constantly are revisiting emergency plans and enhancing practices to more effectively and efficiently communicate in times of crisis. Every institution of higher education has in place some procedures and practices for addressing critical incidents; however, the readiness to apply effective notification procedures and systems varies widely.¹⁴ Technology offers essential tools for communication and can complement the requirement for critical incident management plans to have redundancy in communication.

Social networks offer colleges and universities an inexpensive approach for disseminating messages in a timely manner, maintaining lines of communication throughout the duration of the emergency, and notifying all stakeholders, including students, employees, friends and family, emergency responders and media. Campuses are learning to adapt to social networking as trends change over time.

It is a good practice to assess an institution's tools for communication annually. Social networks offer a viable option for campuses to communicate and can assist with rumor control, two-way and one-way

¹³ U.S. Department of Education, Office of Safe and Drug-Free Schools. 2009. Action guide for emergency management at institutions of higher education. January. Washington, D.C. Available on www.ed.gov/emergencyplan.

¹⁴ Educause, April 2010. "Seven things you should know about emergency notification systems". <https://net.educause.edu/ir/library/pdf/EST1004.pdf>

sharing of information during a critical incident, and providing consistent message. Critical communications components to countering fast-moving rumors and threats of violence threats include:

- State only facts; all information released must be accurate. While there is growing pressure on campus officials to release information quickly in a crisis or in periods of high rumors, accuracy is the most important factor.
- Notifications should be clear and consistent. Campus and police officials should have unified communications so as to send consistent messages. Consistency in the messaging is important.
- Release information in a timely manner at the on-set of the rumors with periodic updates as necessary and appropriate.
- Redundancy of the message matters. Campus administrators and safety officials must send the same information out using multiple tools for communication (such as alert systems, social media, text messaging, campus website, and mass media).
- Have a formal plan for crisis notifications and professionally train your administrators and crisis team members on communicating effectively with media and all stakeholders. Audit crisis communications plans annually and train staff.
- Review policies, student handbooks, employee manuals, code of conducts and discipline policies to make sure they have solid legal and administrative provisions for disciplinary action to address individuals who make threats and are disruptive to the educational environment.
- Campus administration should have proactive discussions about the firm, fair and consistent enforcement of these rules if and when incidents arise.
- Educate students and employees about their role and behavioral expectations related to preventing and reporting rumors and threats of violence, as well as cell phone and text messaging use, especially during an emergency. Members of the campus community need to know that responsible behavior is expected of them, that consequences will occur for inappropriate behavior, and that starting, spreading and fueling rumors are serious offenses that jeopardize safety.
- Inform the members of the campus community about procedures for immediately notifying campus administrators and security personnel of any threats and concerns.

Recommendation #8: Campuses should utilize social media as a proactive tool for notification of emergency situations and adopt policies for such use. Leveraging the same medium where a social media threat is made to address the threat ensures communication with the same potential audience.

Conclusion

Over several months, the task force met amongst itself, with experts in the field, and with major players across the industry, to determine just how best SUNY campuses should be evaluating, addressing, and working to prevent threats – particularly anonymous ones – by way of social media.

Through all of these conversations, one overarching theme rose above the others: social media should be embraced as a positive tool for growth and community. While recognizing there will always be bad players in any arena, it was imperative to the task force members that these recommendations conveyed clearly that it was the duty of the University to implore responsible use of social media, rather than to curtail it in any way.

In fact, it can be said that social media itself represents the best of academia and the university setting. An open, equal exchange of ideas ultimately leading to an intention of progress for both the individual and for society. With that in mind, it is only natural that colleges would embrace this new frontier as an extension of their own mission and purpose.

At the same time, the task force clearly understood higher education's parallel responsibility to provide a safe and nurturing learning environment for students and all who benefit from these educational institutions. This is why preventative education and appropriate response were such a critical aspect of the task force's thinking and are reflected in the final recommendations.

It is the intention that this will truly be a living document. In the scope of human history our comprehension of the effect that worldwide instantaneous communications will have on our behaviors and capabilities is only fractionally understood to date. Today's technologies are sure to be tomorrow's history, and colleges and universities will constantly need to move along with their approaches to these challenges as the landscape changes. It is, however, the belief of this task force that the recommendations included here will prove effective as we all strive to deal with the issues in front of us – not only on our campuses in New York, but hopefully, across the nation.

Appendix A – Summary of Yik Yak Incident at SUNY Canton

On the morning and afternoon of October 22, 2014, a series of terrorist shootings had taken place at Parliament Hill in Ottawa, 75 miles from the SUNY Canton campus. A Canadian soldier on ceremonial duty at the Canadian National War Memorial was killed. The shootings were extensively covered on both the local and national news in Canada and in the United States. This followed a vehicular homicide incident two days earlier, when two Canadian soldiers were run over by a terrorist's car in Saint-Jean-sur-Richelieu, PQ, killing one.

On the evening of October 22, Courtney Bish (Dean of Student Affairs) contacted President Zvi Szafran to inform him that SUNY Canton and St. Lawrence University students were engaged in posting insults and mild threats to each other on Yik Yak. She asked if the College should try to block access to the site. The President, who had never heard of Yik Yak before, gathered information from the web before deciding to not restrict access as an issue of freedom of speech. He noted that articles on the web indicated that in some previous incidents, persons making threats had been successfully traced, despite the purported anonymity of the app.

Just after midnight, SUNY Canton Police Chief John Kaplan was informed of a campus threat that had been posted on Yik Yak. The threat read:

"This is a message to all SUNY Canton students. If you value [sic] your life do not go to class tomorrow, I plan on killing myself but before that I plan on taking as many of you worthless piles of crap, be ready."

Chief Kaplan contacted Dean Bish, who was already aware of the post, since it had been reported to her from Residence Life Director John Kennedy, who had in turn been informed of it by several students.

A preliminary threat analysis was carried out by Dean Bish and Chief Kaplan, concluding that the post did not rise to any level on the College's Emergency Response Resource Group grid. Posts on Yik Yak that receive five negative votes ("downvotes") are automatically removed from the site. While the threat had been taken down due to downvotes within 5 seconds, it had already been seen, screenshots made, and copies transmitted to hundreds of students and family members.

President Szafran, Executive Director of University Relations Lenore VanderZee, and Senior Media Relations Manager Greg Kie were notified of the threat, and it was decided to send out a campus-wide email, acknowledging the College's awareness of the post, and stating that our assessment was that the threat was not credible. At 1:47 AM, other campus officials were informed by email about the threat. At 3:45 AM, SUNY Police Commissioner Bruce McBride and U.S. Department of Homeland Security Special Agent Tim Losito were informed of the threat by email.

At 8:00 AM, SUNY Canton's Executive Cabinet met, with the addition of Lt. Brian Perry, representing the University Police. After a review of the posting and the threat analysis, it was decided to continue classes but to increase police surveillance. A second Executive Cabinet meeting was scheduled for 11:00 AM. A second email from the President was sent to the campus, stating that the threat wasn't credible, classes were continuing, and to expect an update at noon.

Many emails and telephone calls (as well as Yik Yak postings) were received on the campus during this time, the majority critical. People were concerned as to why classes hadn't been cancelled, especially given the terrorist occurrences that had happened recently in Canada. Many felt that if there was any level of risk, classes should have been cancelled. Phone calls were fielded by the Public Relations Office and the President's Office. The earlier campus email messages were reposted on the College's Facebook page. The Campus Police also contacted Yik Yak, asking for their assistance in tracking down the person who had made the threatening post.

President Szafran contacted SUNY's Public Relations, Legal, and the Chancellor's Offices. Chancellor Nancy Zimpher immediately took the call, and after hearing a synopsis of what had happened so far,

assembled her cabinet to review the situation. She also dispatched Commissioner McBride to SUNY Canton.

The 2nd Executive Cabinet meeting was held at 11:30 AM, with Police Chief Kaplan also in attendance. A discussion of what had happened so far took place, with some disagreement about whether the College had reacted appropriately thus far. The strong (though not unanimous) consensus was that we had neither over- nor underreacted. The College's threat analysis procedure was reviewed and discussed.

At 11:45 AM, a new post was uploaded to Yik Yak:

"It's happening at noon."

While it wasn't clear whether the new post was related to the earlier threat, in the interest of safety, the Executive Cabinet immediately to Shelter in Place. A *NY Alert* message was sent out at 11:47 AM, and calls for assistance were made to the Canton Village Police, New York State Police, St. Lawrence County Sheriff's Office, and Homeland Security. An email update was sent to the campus.

At 12:39 PM, a new Yik Yak message was posted:

"Gun spotted on campus"

A command post was established at the University Police Offices. After some discussion, the Executive Cabinet decided to begin clearing the academic buildings on campus, with the occupants to be escorted to the parking lots and off campus or (if they were resident students) to the residence halls. Several staff volunteered to drive the campus vans doing the escorts.

At 1:22 PM, a new Yik Yak message was posted:

"Anyone else in Smith East [a residence hall] hearing loud shit?"

At 1:24 PM, F.B.I. Special Agent Mark Parks called the campus, and agreed to ask the Behavior Analysis Unit to examine the threats. The College's actions thus far were supported. At 1:29 PM, a new Yik Yak message was posted:

"Was there shots fired in the Library?"

Calls to the Library indicated nothing unusual. A campus email was sent at 2:00 PM stating that no incidents had been reported so far, and describing the evacuation process in general terms. The evacuation began soon after, with additional NY Alerts and emails sent on an hourly basis. Discussion continued in the Executive Cabinet about the duration of the lockdown, and how it might be lifted. Chief Kaplan joined a conference call with the SUNY system. Various support phone calls began to come in, including an offer of assistance from St. Lawrence University, and messages of support from NY Senator Patty Ritchie and Canton Village mayor Mary Ann Ashley. Social media messages began to turn positive during this period, with several messages received of both a serious (asking for help securing needed medicines) and less serious (wondering when the lockdown would be lifted since the sender was getting hungry) nature.

During the final stages of clearing the academic buildings, planning began between Deputy Chief Tim Ashley and the residence hall directors to carry out a safety sweep of the residence halls. The College's Counseling Staff were asked to stay on campus in case they were needed. The sweep began at 4:00 PM. Once the all clear would be announced, the College wanted to feed all the residence hall students simultaneously, in the residence halls. Since delivering so many meals simultaneously was beyond the capacity of our campus food service, arrangements were made with St. Lawrence University's Food Services to bring 300 additional meals to the campus and help deliver them. The *All Clear* was given at 6:45 PM.

The press had been held off campus throughout the lockdown, with periodic updates provided by the College's public relations staff. After the *All Clear* was announced, President Szafran, Chief Kaplan, Commissioner McBride, and the public relations staff met with the press, gave a brief update, and answered all questions. The Executive Cabinet met with the students in the residence halls to ensure that they had eaten, were in good spirits, and that there were no ongoing issues. At 11:00 PM, a final email was sent to the campus, thanking the community for its cooperation and patience, thanking the police agencies, and stating that the campus was safe.

Classes resumed on Friday, October 24. Some negative emails and calls continued, questioning the College's reopening when the threat-poster hadn't yet been caught. The next day, the Campus Police informed President Szafran and Executive Director of University Relations VanderZee that the person had been identified and arrested. Announcements were immediately sent to the campus and media.

On Monday, October 27, President Szafran held open forums separately for the faculty, staff, and students so that each group could ask any questions or raise any issues they thought appropriate. A summary of the events and how decisions were made was sent to the campus on October 28 in the President's weekly blog.

Appendix B – Proposed Board of Trustees Resolution

DRAFT

MEMORANDUM

November 5, 2015

TO: Members of the Board of Trustees

FROM: Nancy L. Zimpher, Chancellor

SUBJECT: Recommendations of the Chancellor's Task Force on Social Media Responsibility

Action Requested

The proposed resolution asks the Chancellor and her staff to implement the recommendations of the Task Force on Social Media Responsibility across the 64 SUNY campuses.

Resolution

I recommend that the Board of Trustees adopt the following resolution:

Whereas, incidents related to anonymous social networks have been making headlines as schools and colleges see an increase of occurrences; and

Whereas, in light of recent experiences at several SUNY campuses, a Chancellor's Task Force on Social Media Responsibility was established; and

Whereas, the charge to the Task Force was to develop system-wide recommendations on tackling issues related to social media responsibility; and

Whereas, the Task Force, consisting of experts in the field, was to consider strategies for improving social media responsibility on campuses, across two overarching principles of education and response,

Be it resolved, that the State University of New York Board of Trustees hereby adopts the Task Force's eight recommendation across all campuses, including:

Recommendation 1: Universities should treat social media primarily as a positive tool and not try to restrict its use.

Recommendation 2: Digital citizenship is a necessary element in any contemporary university curriculum. Students should learn that social media can be an important tool in building a supportive community and that a permanent, public digital footprint is created from their participation.

Recommendation 3: Each university should incorporate social media policy into its existing campus social policies and student codes of behavior, following the same consultative and transparent procedures that developed the earlier policies.

Recommendation 4: All campuses should develop and communicate a process for community members to report concerns regarding social media content so that it can be assessed and handled by the institution.

Recommendation 5: Each university should provide instruction to students in an appropriate place in the curriculum (such as first-year orientation courses or programs) on how to maintain a professional digital identity. Students should be informed that all illegal activity, even if perpetuated on a theoretically anonymous or ephemeral platform, can be prosecuted and carry consequences.

Recommendation 6: Each university should provide training to faculty and relevant staff in appropriate use of social media. A system-wide MOOC on “Social Media and College” and e-Citizenship campaign should be created for this purpose.

Recommendation #7: Campuses should collaborate in developing a well prepared social media policy, code of conduct, and training program. In addition, campuses within the system should know what other campuses might be available to assist with monitoring social media activity in the aftermath of a campus critical incident.

Recommendation #8: Campuses should utilize social media as a proactive tool for notification of emergency situations and adopt policies for such use. Leveraging the same medium where a social media threat is made to address the threat ensures communication with the same potential audience.

and,

Be it resolved, that these recommendations will be implemented by all SUNY campuses by June 1, 2016, and

Be it resolved, that SUNY System Administration will develop resources and websites to assist campuses in rolling out the new educational initiatives needed to implement the recommendations, and

Be it resolved, that SUNY System Administration will explore the possibility of using a cross-campus social media management solution not for the purposes of monitoring but rather for collaboration, and

Finally, be it further resolved, that the Chancellor or a designee shall oversee the implementation of these recommendations with appropriate communication to presidents and students.