



MEMORANDUM

June 22, 2016

TO: Members of the Board of Trustees

FROM: Nancy L. Zimpher, Chancellor

SUBJECT: Social Media Responsibility: Task Force Recommendations

Action Requested

The proposed resolution approves the eight recommendations of the Chancellor's Task Force on Social Media Responsibility and encourages campuses to adopt practices consistent with the recommendations.

Resolution

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

Whereas the proliferation of anonymous social networks has resulted in an increase in internet-based threats of violence in schools and on college campuses across the country; and

Whereas the campuses of the State University of New York have experienced first-hand the effects of such internet-based threats of violence; and

Whereas as a result of such incidents, the Chancellor called for the establishment of a Task Force on Social Media Responsibility ("Task Force") to develop, under the overarching principles of education and response, best practices with regard to social media responsibility; and

Whereas the Task Force was comprised of experts in the field of digital media as well as with representatives from across the SUNY community; and

Whereas the Task Force prepared a comprehensive report containing eight specific recommendations

("Recommendations") which demonstrate best practices for implementing responsible social media practices; now, therefore, be it

Resolved that the Board of Trustees hereby approves the following recommendations set forth by the Task Force:

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 community. Students should be made aware 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: Campuses should incorporate social media policy into their existing campus social policies and student codes of conduct, following the same consultative and transparent procedures that developed the earlier policies.

Recommendation 4: Campuses should make their communities aware that reporting concerns regarding social media content so that it can be assessed and addressed by the institution works in the same way as reporting concerns in a non-digital setting.

Recommendation 5: Campuses should familiarize students at appropriate junctures 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: Campuses should make available training resources to faculty and relevant staff in appropriate use of social media. System Administration will work with campuses to encourage innovation and the sharing of tools, programs, and content.

Recommendation #7: Campuses should collaborate in developing training programs and policies dealing with social media, integrating where possible with their code of conduct. 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 further

Resolved that all State-operated and community college campuses are strongly encouraged to incorporate the best practices set forth in the Recommendations into their campus policies; and, be it further

Resolved that System Administration will develop resources and websites to assist campuses in rolling out educational initiatives needed to implement the best practices set forth in the Recommendations.

Background

The proliferation of anonymous social media networks has resulted in a rise in anonymous threats of violence on college campuses across the nation, including on SUNY campuses. Perhaps the most notorious of these incidents occurred at SUNY Canton in October 2014 in which an anonymous Yik Yak poster threatened to take his/her own life and as well as the lives of others. A similar incident followed in November 2014 when an anonymous Yik Yak poster threatened to detonate an explosive device on the University at Albany campus. These incidents are merely representative of a troubling national trend in the misuse of social media.

As a result of these incidents, in December 2014, Chancellor Zimpher called for the establishment of a Task Force on Social Media Responsibility, to be co-chaired by SUNY Canton President Zvi Szafran and Rachel Hot, New York State's Chief Digital Officer. The Task Force was charged with developing system-wide recommendations around education to prevent social media abuse, and guidance on how to respond to social media threats. The task force was comprised of experts in digital media as well with representatives from across the SUNY community, including campus administration, student affairs, faculty, law enforcement, legal, technology, and students. The Task Force prepared a report, which contains the Recommendations noted above. A copy of the report is on file with the Office of the Secretary.



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 best practice 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 proliferation of collaborative internet applications and platforms for the purpose of sharing information, 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.

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, Instagram, and Tumblr. 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 B]**

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}

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

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/>

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
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

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/>

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	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 Trustees 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

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

The internet is 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, and promote health. One of the most positive things about social media is that it has democratized the internet. 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 2: Digital citizenship is a necessary element in any contemporary university community. Students should be made aware 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.

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 3: Campuses 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.

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 promote amongst our students, faculty, and staff to encourage responsible behavior and support positive use of social media?

Given the ubiquitous nature of social media, the Task Force concluded that every university should have policies pertaining to social media use and responsibility, 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 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

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

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. 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 4: Campuses should make their communities aware that reporting concerns regarding social media content so that it can be assessed and addressed by the institution works in the same way as reporting concerns in a non-digital setting.

“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. Existing “Acceptable Use Policies” may already address some of this scope.

Recommendation 5: Campuses should familiarize students at appropriate junctures 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.

Education is a critical tool for SUNY institutions to maximize the positive use and minimize the negative use of social media on their campuses, and should 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.⁸

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.

⁸ 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>

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.

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.

Recommendation 6: Campuses should make available training resources to faculty and relevant staff in appropriate use of social media. System Administration will work with campuses to encourage innovation and the sharing of tools, programs, and content.

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.

Faculty create digital identities in two common ways: first, as an educator interacting with students and second, like staff do, 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.

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 are included in this reminder.

Recommendation #7: Campuses should collaborate in developing training programs and policies dealing with social media, integrating where possible with

their code of conduct. 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.

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.^{9 10} 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).

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. In doing so, colleges should utilize best practices not only from across the nation but also take advantage of being part of the SUNY system and work with colleagues across the state to meet the needs of our campuses.

Critical incident management planning must consider the reactionary, impulsive and spontaneous nature of interactions on social networks. When planning, managers 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.

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 #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.

Institutions of higher education are constantly 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.¹¹ 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.

⁹ 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.

¹⁰ 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.

¹¹ Educause, April 2010. "Seven things you should know about emergency notification systems". <https://net.educause.edu/ir/library/pdf/EST1004.pdf>

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 sharing of information during a critical incident, and providing consistent message.

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 – Suggestions for 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.

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.

Appendix B – 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 decided 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.