TEACHING ONLINE SAFETY:

TIPS, TRICKS, AND BEST PRACTICES FOR ONLINE SAFETY EDUCATION

Aynsley Pescitelli (M.A.)
(PhD Student, Simon Fraser University School of Criminology)

&

Merlyn Horton
(Executive Director, Safe Online Outreach Society)

Abstract:
The focus of this paper is on best practices for online safety education. While research in this area is still in development, the literature contains several promising tactics and examples from which to draw from. Areas of recent focus include definitional difficulties, the importance of digital citizenship, the role of empathy, encouraging bystanders to become active participants, enforcing positive cyber norms, tips for introducing, developing, and continuing online safety education, and the importance of evaluation.

Keywords: online safety education; cyber safety; cyber education; online education; Internet education

Introduction

Cyber safety is currently a hot topic; one needs only to tune into the nightly news, open the pages of a newspaper, or check the online feeds to encounter shocking stories of online harm and cruelty. Though these stories are not the norm, this does not make them any less concerning nor the need for online safety education any less pressing. While it is clear that education of some kind is needed, "very little is currently known about what works to educate youth about cyberbullying and online safety" (Hinduja & Patchin, 2009, p. 143). Though the research in this area is somewhat sparse, it is important to address such gaps in the literature and attempt to address and fill them. With this in mind, the following paper examines the current research on best practices in online safety education.

To begin, this paper addresses definitional inconsistencies and the importance of avoiding labelling and misconceptions about online behaviour. The topic of digital citizenship and its role in a comprehensive cyber education program is covered next, including the nine key elements of an effective digital citizenship curriculum. This is followed by a discussion of the importance of empathy development in online and offline settings, as well as the role of bystanders in online activities. This leads to cyber norms and the potential to engender prosocial ones to replace current negative, biased, or misconstrued norms. Tips for incorporating cyber safety into the curriculum and when to start are provided next, and the idea of students as experts and peer educators is also covered. This leads into the importance of understanding and preserving online evidence, and some helpful teaching tips and examples are provided based on the literature. Finally, the importance of educational program evaluation is addressed, with some examples of potential evaluative mechanisms.

Definitions: Be Clear and Explicit, but Avoid Misconceptions and Labelling

While terms such as cyberbullying, cyberharassment, cybervictimization, and cyberaggression can be useful for teaching certain aspects of Internet safety, they can also confuse students. Individuals do not always identify their own experiences within these categories and their associated definitions. Additionally, there is definitional overlap that can lead to further confusion. Some researchers stress that terms such as cyberbullying and cyberharassment can be used interchangeably (Beran & Li, 2005; Strom & Strom, 2005), while others argue that such terms, while similar, should have different definitions (Kowalski, Limber & Agatston, 2012; Hinduja & Patchin, 2009). It is no real surprise that, if researchers cannot even agree on a universal definition for such behaviours (Langos, 2012), students cannot easily place their actions and experiences within these categories. Thus it can be helpful to use general or alternative terms and to avoid charged language and labelling.

A substitute term that encompasses a great deal of problematic online behaviour is *cyber drama*. Coined by *Microsoft* researcher danah boyd, online drama is distinct from other oft-used terms. Drama allows for harmful online interactions involving complicated conflicts with a muddled distinction between victim and perpetrator (Bazelon, 2013). "Drama is the language that teens—most notably girls—use to describe a host of activities and practices ranging from gossip, flirting, arguing, and joking to more serious issues of jealousy, ostracization, and name-calling" (Marwick & boyd, 2011, p. 2). More importantly, regardless of whether terms such as bullying, harassment, and aggression apply, such words are often not part of adolescents' everyday vocabulary. Interestingly, actions that teens refer to as drama may be perceived by adults and outside parties as bullying. This distinction allows individuals to experience drama without explicitly accepting the identity of bully or victim (Marwick & boyd, 2011).

Introducing specific terms can be problematic, particularly if students have misconceptions about such terms or if the definitions have negative connotations. This leads to the concerns about labelling, as very few students will willingly take on the label of bully or harasser. Similarly, terms such as victim can also lead to similar resistance. Individuals are more than their isolated behaviours, and terms that are so emotionally charged and negative are not likely to appeal to many students, even if their actions fit within the definitions. These terms are highly stigmatized, and may lead young people to deny their actions rather than discuss them openly and attempt to learn from them (Bazelon, 2013).

Beyond Cybervictimization: Teaching Students to be Responsible Digital Citizens

Although teaching students about cyber risks is important, it is pivotal to address all aspects of Internet use to encourage the development of well-rounded and responsible student users. It is in this area where the teaching of digital citizenship is

key. "Digital citizenship aims to teach everyone (not just children) what technology users must understand in order to use digital technologies effectively and appropriately" (Ribble, 2011, p. 10). There are nine basic tenets of digital citizenship, and efforts should be made to incorporate each of these into online safety programs. The nine elements include: digital access, digital literacy, digital communication, digital etiquette, digital commerce, digital security, digital rights and responsibilities, digital law, and digital health and wellness (Tan, 2011; Ribble, 2011).

Digital access relates to the ability to fully participate in online society. Though it may appear that the youth of today have access to many digital tools and locations, everyone does not have equal access (Ribble, 2011). It is thus important to encourage at-school use of technology in appropriate settings. This also ties into the importance of digital literacy. For students to use technology safely and to the best of their abilities education is key (Tan, 2011; Ribble, 2011). Keeping up with developments and new technology is pivotal (Tan, 2011), as is learning from students about their personal use of technology. While technology-based education is becoming increasingly common, "learning with technology does not always include instruction on appropriate and inappropriate use" (Ribble, 2011, p. 26). It is thus important to also include discussions surrounding broader uses of the technology and what constitutes acceptable and unacceptable use.

Another issue related to digital access is that of digital communication. In the digital age, 24/7/365 access has become the norm, and communication is possible at all hours of the day (Tan, 2011). There are also countless online communication options and tools, with mobile devices allowing an even greater level of accessibility. Such access is clearly exciting and convenient, but education needs to stress appropriate digital communication tactics to ensure that students fully appreciate the related risks. Digital communication education should emphasize the permanence of online

conversations and posts, and also the importance of how communications might be interpreted by the intended recipient and others (Ribble, 2011).

When engaging in online communication, students need to also think about the role of digital etiquette (Kowalski et al., 2012; Whitson, 2012).

> In the past it was up to parents and families to teach basic etiquette to their children before they reached school. The problem with the new technologies is that parents have not yet been informed about what is appropriate and what is not. (Ribble, 2011, p. 29)

If students are not taught appropriate digital etiquette, or *netiquette*, before entering a school setting it is crucial to introduce these topics as early as possible. Netiquette education should involve discussions about respecting other online citizens and considering the consequences of online actions (Ribble, 2011).

Teaching students about digital commerce requires introducing topics related to online consumerism (Tan, 2011). This can be a difficult aspect to teach, as teachers may have trouble incorporating it into the wider curriculum or may feel that it is not their responsibility to cover it (Ribble, 2011). It is, however, important to think about how electronic selling and purchasing relate to other issues of online safety. For example, releasing financial and personal information online can put individuals at risk of identity theft and online scams (Ribble, 2011). Teaching students to be aware of what they are sharing as well as how to determine if sites are safe and reputable is not only important, but it can help raise awareness of good practices for online information sharing and privacy. Discussions of online buying and selling relate well to the topic of digital security. Digital security lessons should stress the importance of protecting oneself online (Ribble, 2011; Tan, 2011). This includes self-protection from potential harms such as online harassment, stalking, phishing, viruses, hacking, and identity and information theft (Ribble, 2011).

Digital rights and responsibilities revolve around freedoms and restrictions in the digital sphere. These rights and responsibilities extend to all Internet users, with the most basic of rights including the right to online privacy and the right to free online

speech (Tan, 2011). Discussions of rights and responsibilities should cover academic integrity, plagiarism, and the ethical use of online information, as well as harassment, threats, and destroying others' online content (Ribble, 2011). Digital law education also relates to online rights and responsibilities, but does so in a more explicit fashion. This includes teaching students about online actions that are criminal in both online and offline contexts (Tan, 2011; Ribble, 2011).

Finally, a very important issue that needs to be addressed in online education is that of digital health and wellness. Students need to understand how Internet use and online actions can lead to serious physiological and psychological effects, both for themselves and others. Examples include Internet addiction, eyestrain, headaches, and repetitive stress injuries (Tan, 2011; Ribble, 2011).

The Internet is Real Life: The Role of Empathy in Online Education

A promising way to address harmful online activities directed at other individuals is to stress the importance of empathy, both on and offline. Empathy is sometimes confused with sympathy, but it is a distinct concept. "Empathy is the actual understanding of how another feels- the capacity to walk in another's shoes" (Berkowicz & Myers, 2013, para 4). Developing online empathy can be difficult for several reasons, including: delay in response, inability to see reactions firsthand, perceived lack of consequences, the role of disinhibition, and the tendency to create a distinction between online and offline activities.

Online reactions and responses are not received in the same fashion as they are in person. Responses to messages can occur in real time or much later, which can separate individuals from their actions when they do not receive an immediate response (Reeckman, 2009; Hinduja & Patchin, 2009). Additionally, emotional responses are not experienced as powerfully as they are face-to-face (Mesch, 2009; Kowalski et al., 2012). On the Internet, users are generally not exposed to facial cues, tone of voice, and eye

contact (Bazelon, 2013). "When a person uses hurtful words in real life, the speaker can generally see the effect right away; but in cyberspace, no swift response shows the appropriateness or inappropriateness of his or her actions" (Hinduja & Patchin, 2011, p. 49). Thus individuals have to work harder to think about the consequences of their online interactions. This also ties into the concept of disinihibition, which allows individuals "to be freed from the restraints on [their] behavio[u]r" (Hinduja & Patchin, 2009, p. 21). Perceptions related to the inability to be identified online, lack of evidence, and anonymity may allow people to more easily engage in risky or harmful online activities (Kowalski et al., 2012).

One of the biggest issues in teaching online empathy is the oft-employed distinction between the Internet and "real life." Many Internet users distinguish between their online and offline activities by employing the term "IRL" to identify their offline lives (Pescitelli, 2013). We need to work hard to break down the myth of IRL and to teach young Internet users that everything they do online is in real life. Online activities occur in real life and have real life consequences, so it is important to use terms like "offline" and "in person" when discussing non-Internet activities. This can encourage the consideration of online and offline consequences following online actions, and can further encourage the development of empathy.

Bystanders: Don't Just Sit Back and Let it Happen

Though most students do not engage in harmful online activities, many do witness online victimization of peers and other Internet users. It is important to teach young people that they have power as witnesses to such behaviour, and that they are not stuck in a passive bystander position. Students need to realize that "by doing *nothing* they are doing *something*" (Hinduja & Patchin, 2009, p. 174). When individuals are exposed to hurtful online speech and actions, having an audience witness these actions can lead to further harm. The presence of an audience is particularly

problematic when bystanders join in (Kowalski et al., 2012), but can also be an issue when other users say nothing at all. While it is important for students to escape the bystander role, it is understandable that many are reluctant to stand up for others in online settings. Being supportive does not necessarily entail confrontation or conflict (Bazelon, 2013). Alternatives include sending a personal email or instant message to individuals in need of support. If students also have an offline relationship with the individual it can be useful to approach them privately at school or in-person to offer help and to stress that the behaviour was inappropriate and is not tolerated by others. Finally, if the online actions are particularly troubling it may be useful to report them to a trustworthy adult (Kowalski et al., 2012; Hinduja & Patchin, 2009).

Cyber Norms: Enforcing Prosocial Norms and Eliminating Misconceptions

Though it can be tempting to introduce controversial cases and examples to illustrate the importance of online safety, a better educational tactic is to draw attention to others making good online decisions. It is important to teach students that responsible online activities are the norm, regardless of coverage in the media and popular culture (Patchin & Hinduja, 2012; Bazelon, 2013; Kowalski et al., 2012). The key is to introduce and reinforce positive online norms, and to also discuss some of the wider societal misconceptions surrounding online behaviour. It is important to "reinforce positive norms by showing that the majority of young people make safe and responsible decisions using digital technologies and that they disapprove of hurtful behavio[u]r" (Willard, 2012, p. 86). It can be helpful to include peers in this process, either by having them present or work with other students and talk about prosocial online behaviour (Kowalski et al., 2012). Adult role models can drive the message even further home, particularly teachers, administrative staff, family members, and members of the wider community (Kowalski et al., 2012). Finally, survey data (school-based, local, national, or international) can be an excellent way to display information about prosocial

online values; when students see that large numbers of other students are not engaging in harmful behaviour the messages can be even more effective (Kowalski et al., 2012).

Two Birds, One Stone: Incorporating Cyber Education into the Curriculum

It is important to incorporate cyber safety education into the regular curriculum rather than simply addressing it once per year in an obligatory session. A great way to do this is to address cyber topics in related discussions in other classes (Butler, 2010; Patchin and Hinduja, 2012; Beale & Hall, 2007). For example, discussions of cyberbullying and harassment fit nicely with lessons based around in-person bullying and harassment (Hinduja & Patchin, 2011; Hinduja & Patchin, 2009). Lessons related to appropriate Internet use and safety can be both useful and relevant in classes that include Internet-based activities. This allows students to safely use the classroom technology employing a hands-on approach. While this is both helpful and directly relevant, it is especially useful to incorporate the same technologies used by students in non-school (Ribble, 2011). Integrating these lessons into several aspects of the curriculum allows for multiple opportunities to enforce and reinforce positive online norms and to address issues of concern.

Start Young, But it is Never Too Late

In today's digital society, children are beginning to use the Internet at much younger ages (Mishna, Saini & Solomon, 2009). Understandably, this means that cyber education needs to start as early as possible. Cyber safety lessons are often a focus at the middle and high school level, as these years are often associated with high levels of cyberbullying and related activities (Kowalski at al., 2012; Hinduja & Patchin, 2009). Ideally, online behaviour education should start in primary school or even sooner (Butler, 2010). The earlier consistent safety messages are provided, the more likely it is that such messages will sink in (Kowalski et al., 2012). Hinduja and Patchin (2009)

"encourage introducing the topic as early as possible- and definitely before [children] start exploring the Internet alone" (p. 129). Lessons can start small, and it is important to introduce the topic in an age-appropriate manner (Kowalski et al., 2012). Once the topic has been raised, there is potential to build on previous lessons and delve into specific concepts in greater detail. Though it is important to start early, it is never too late to introduce the topic of online safety (Hinduja & Patchin, 2009). The topic can and should be covered at all levels of education, including middle, high school, and even in post-secondary settings.

Youth Centred and Led: Peer Education and Students as Experts

One of the biggest problems with much current online education is that teachers often know less about the technology being covered than their students do. While students have been raised with the Internet and have not known a world without it, most adults do not share this comfort level (Keith & Martin, 2005; Kowalski et al, 2012; Baggio & Beldarrain, 2011). Thus it is not only difficult for educators to remain on top of cyber developments and trends, but the perception of lack of adult cyber knowledge can lead to issues in gaining credibility and developing rapport with students. "It is imperative that parents, teachers, practitioners, and researchers neither overlook nor underestimate children's knowledge of computers and of the Internet" (Mishna et al., 2009, p. 1226). Therefore it can be very helpful to learn from our students and to consider peer cyber education options.

Since students are generally on top of technological trends and popular sites, these individuals can be an invaluable resource (Ohler, 2012). The trendiest sites are ever changing, and adults always seem to be at least one step behind (Kowalski et al., 2012). Kowalski et al. (2012) encourage the use of a teen expert panel as a way to keep up with popular online uses, abuses, and settings. Allowing students to provide feedback and examples can help to shape programs and keep them current.

Additionally, student involvement can lead to increased investment and participation in such programs, as participants see that their voices are being heard and that their opinions are valued (Ohler, 2012).

Peer-led cyber education can also be very useful in this regard. "The peer group often has more legitimacy than the teacher in addressing social issues, so making use of student leaders to help teach lessons on social Web safety and cyberbullying is a great prevention strategy" (Kowalski et al., 2012). Peer leaders can be from the same age group or older groups of students. Older student mentors (generally high school students) may be especially influential, as younger students often look up to them, seeking their approval (Hinduja & Patchin, 2009; Bhat, 2008; Kowalski et al., 2012). It may be easier for students to relate to others who are close to their own age and who can understand what they are going through. Adult educators can incorporate peer leaders into their lessons by allowing them to take the lead and encourage peer-based discussions rather than simply lecturing from the front of the room (Willard, 2012).

Online Evidence: What Happens on the Internet Stays on the Internet, for Better or Worse

It is important to discuss issues specific to online forms of evidence, as the permanence of online information can serve to be both a strength and a weakness. For those who have been victimized online, discussions about online evidence should include saving such items in the event that the behaviour continues or worsens (Hinduja & Patchin, 2009; Kowalski et al., 2012). Evidence can be saved by taking screenshots, printing copies of the screen, saving copies of emails, and saving online discussions and events as files (Kowalski et al., 2012). It is also important to keep track of dates, times, and locations of incidents as they occur (Kowalski et al., 2012).

Since the permanence factor can be useful for forming a case against a cybervictimizer, it can understandably also lead to problems for all Internet users. Even

when not victimizing others online, students often post material that they would not want future employers or family members to see. It is important to stress that online activities leave a *digital footprint* that can be traced and followed (Hinduja & Patchin, 2009). It is also key to address online privacy by discussing settings on various sites (Hinduja & Patchin, 2009). Finally, students should be taught that even when they do delete text, photographs, or videos, once they are publicly available online there is no guarantee that they have not been archived or replicated by other users (Hinduja & Patchin, 2009).

Where Do We Go From Here?: Some Helpful Teaching Tips and Examples

What works with one group may not work with another, and it is important to keep age, needs, and technological aptitude and experience in mind when designing cyber education programs. Still, there is no need to re-invent the wheel; we can learn from other educators and researchers and adapt their strategies for use with different populations. Here are some interesting and potentially useful examples drawn from the literature:

- Sponsor presentations and assemblies (Hinduja & Patchin, 2009; Patchin & Hinduja, 2012)

    While regular, curriculum-based cyber education is ideal, assemblies and presentations can be an excellent way of reaching a large number of people (e.g. the entire student body, all educators and administrators, parents, or an entire grade) quickly and easily. Presentations can also be an effective way to introduce the topic generally and to later expand on some of the points raised. Furthermore, presentations can be a great way to introduce new or interesting topics that have not yet been covered as part of the regular curriculum. For assemblies to be most effective, topics should be "relevant, hard-hitting, and meaningful" (Patchin & Hinduja, 2012, p. 8).

- Encouraging problem-solving and presenting scenarios (Hinduja & Patchin, 2009)

   Teaching students to be good problem solvers and to take accountability for their actions is helpful in many regards, but it can also be useful when teaching online safety. This can be done by presenting students with multiple cyber scenarios and asking them to share their solutions with the larger group. Solutions can be generated alone or brainstormed with others in smaller groups. Working together and sharing perspectives is key here, as it can help reinforce positive online norms related to responsible behaviour (Kowalski et al., 2012). Students can also be encouraged to share personal experiences (if comfortable doing so), and the group can then brainstorm appropriate responses to such situations (Hinduja & Patchin, 2011).

- Bring in experts from the community (Hinduja & Patchin, 2009)

   Inviting educators in from other community settings can be beneficial, as these individuals are typically well informed about the specifics of the areas in which they work. Researchers and community groups with expertise in the online arena may be able to provide up-to-date and useful information. School resource and law enforcement officers can assist in discussions about responsible online practices, and can be especially helpful in providing information surrounding laws and legal consequences of online actions. "Officers should also discuss the ways in which online deviance is investigated, so students recognize that just about everything is traceable when sent or posted electronically" (Hinduja & Patchin, 2009, p. 154).

- Assignments and discussions encouraging development of empathy (Kowalski et al., 2012)

Similarly to discussions and assignments encouraging problem solving, educators can introduce lessons that address empathy building as a major aspect. Examples include presenting scenarios and encouraging students to take on the role of different players in the scenario. This can also include discussions of bystanders and their role (Kowalski et al., 2012). Role-playing exercises can be particularly helpful in this regard, and following exercises with group discussions can help to emphasize fundamental points. In individual-based projects, "teachers can develop writing assignments where students take the perspective of someone who is experiencing bullying or cyberbullying behavio[u]r and discuss reactions to the bullying behavio[u]r" (Kowalski et al., 2012, p. 167).

Evaluation is Key

As has been discussed, there is not a single agreed-upon method for teaching online safety effectively. There are multiple promising options, but to determine whether something is working it is important to evaluate programming regularly. "Whatever approach you take, it is essential to conduct a formal and systemic evaluation of its merits so that others can learn from your experience" (Hinduja & Patchin, 2009). It may be useful to administer surveys following cyber safety sessions to gauge student satisfaction with the experience. Including open-ended response options can be beneficial to get additional information such as suggestions for future topics and strategies, and to learn what worked and what did not.

Conclusion

The available literature points to some promising areas where online safety education is developing and, in some cases, thriving. Most of these topics and skills are also applicable and important in offline contexts, lending them well to integration within the wider curriculum. While these tips and examples are a good starting point, there is

much more work to be done. Cyber educators and researchers need to learn what works and what does not. Researchers, educators, and administrators should work together to develop strong evaluative instruments and to make the results of their evaluations available to other interested parties. Cyber safety programs can only be strengthened through trial, error, and research, and the ultimate goal should be to provide the best online safety education possible for this and future generations,

References

Baggio, B., & Beldarrain, Y. (2011). *Anonymity and learning in digitally mediated communications: Authenticity and trust in cyber education*. Hershey, PA: Information Science Reference.

Bazelon, E. (2013). *Sticks and stones: Defeating the culture of bullying and rediscovering the power of character and empathy*. New York, NY: Random House, Inc.

Beale, A. V., & Hall, K. R. (2007). Cyberbullying: What school administrators (and parents) can do. *The Clearing House, 81*(1), 8-12. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=27957591&site=ehost-live

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*(3), 265-277.

Berkowicz, J., & Myers, A. (2013, July 4). A call for empathetic schools. *Education Week*. Retrieved from http://blogs.edweek.org/edweek/leadership_360/2013/07/a_call-for-empathetic_schools.html

Bhat, C. S. (2008). Cyber bullying: Overview and strategies for school counsellors, guidance officers, and all school personnel. *Australian Journal of Guidance and Counselling, 18*(1), 53-66.doi: 10.1375/ajgc.18.1.53

Butler, K. (2010). Cybersafety in the classroom. *District Administration. 46*(6), 53-37. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost. com/login.aspx?direct=true&db=aph&AN=51378367&site=ehost-live

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Corwin Press.

Hinduja, S., & Patchin, J. W. (2011). High-tech cruelty. *Educational Leadership, 68*(5), 48-52. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search. ebscohost.com/login.aspx?direct=true&db=aph&AN=58108039&site=ehost-live

Keith, S., & Martin, M. E. (2005). Cyber-bullying: Creating a culture of respect in a cyber world. *Reclaiming Children and Youth, 13*(4), 224-228. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=16176365&site=ehost-live

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed.). West Sussex, UK: John Wiley & Sons, Ltd.

Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking, 15*(6), 285-289. doi: 10.1089/cyber.2011.0588

Marwick, A., & boyd, d. (2011). *The Drama! Teen Conflict, Gossip, and Bullying in Networked Publics.* Retrieved from http://www.danah.org/papers/.

Mesch, G. S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychology & Behavior, 12*(4), 387-393. doi: 10.1089/cpb.2009.0068

Mishna, F., Saini, M., & Solomon, S. (2009). Ongoing and online: Children and youth's perceptions of cyber bullying. *Children & Youth Services Review, 31*, 1222-1228. doi: 10.1016/j.childyouth.2009.05.004

Ohler, J. (2012). Digital citizenship means character education for the digital age. *The Education Digest, 77*(8) 14-17. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=83515505&site=ehost-live

Patchin, J. W., & Hinduja, S. (2012). School-based efforts to prevent cyberbullying. *The Prevention Researcher, 19*(3), 7-9. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=83626699&site=ehost-live

Pescitelli, A. (2013). *MySpace or Yours?: Homophobic and Transphobic Bullying in Cyberspace* (Unpublished master's thesis). Simon Fraser University, Burnaby, BC.

Reeckman, B., & Cannard, L. (2009). Cyberbullying: A TAFE perspective. *Youth Studies Australia, 28*(2), 41-49. Retrieved from http://proxy.lib.sfu.ca/login?url= http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=42733968&site=ehost-live

Ribble, M. (2011). *Digital citizenship in schools* (2nd ed.). Washington, DC: International Society for Technology in Education.

Strom, P. S., & Strom, R. D. (2005). When teens turn cyberbullies. *Education Digest, 71*(4), 35-41.

Tan, T. (2011). Educating digital citizens. *Leadership, 41*(1), 30-32. Retrieved from http://proxy.lib.sfu.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=87052584&site=ehost-live

Willard, M. (2012). Protecting children in the 21st century. *District Administration, 34*(3), 86-87. Retrieved from http://www.jstor.org.proxy.lib.sfu.ca/stable/25740296