

Lessons Learned about Schools and Their Responsibility to Foster Safety Online

Michael J. Berson, Ph.D.
University of South Florida
Tampa, Florida
United States

Abstract

The Internet has provided an expansive environment that enhances many existing teaching and learning approaches while facilitating new activities that are free of traditional constraints. As a result of the potential for instantaneous interaction without regard for geographic, political, racial, social, and gendered borders, an increased amount of activity is taking place online. In school settings, the need to regulate behaviors in cyberspace and minimize potential and actual risks to children has necessitated some governance over harmful interactions. Two recent cases in the United States will illustrate the emerging struggles of school systems to ensure the safety of youth online.

1 Introduction

The opportunities to expand educational experiences, develop creativity, and foster communication in a global context are among the exciting potential applications of technology; however, these benefits are accompanied by challenges. Most significant among the difficulties are the online risks to safety and emotional well being. Children typically are naïve regarding dangers in cyberspace, and parents often lack familiarity with mechanisms to address these concerns (Berson, Berson, & Ferron, in press; Berson, 2000a). Consequently, educators have an important role to play in addressing the lapse in preventative intervention to create and maintain awareness and safety for young people online.

The safety and well being of children is of paramount importance to educators; however, the reality of practice is that few professionals are prepared for their role as protectors and advocates for children. As children and youth increase the time they spend online they also are progressively immersed in an environment that often has been shielded from the oversight and supervision of parents and other significant adults (Cole et al., 2001). In a medium devoid of standards for conduct and codes of ethics, many young people falter in the quality of their online interactions with others, demonstrating instead a paucity of respect, responsibility, honesty, kindness, justice, or tolerance (Willard, 2000).

The guidance of teachers may assist students in making informed decisions and allow them to demonstrate an ability to apply online critical thinking skills and productive social participation. Although many young people have some awareness of cybersafety as a result of initial discussions with adults, there appears to be a paucity of ongoing communication, leaving adults generally unaware of the online behaviors of children in their care. This is described by Young (1998) as a benign neglect of children's Internet activity.

The distancing of adults from youth as a result of a communication gap and technological divide highlights the shared responsibility of educators in making sure that children have access to and are safely guided through the Internet. The role of educators in promoting

awareness of potential harm and the importance of safe and ethical conduct online is an essential preventative mechanism to counter cyber misconduct. The Internet presents new teaching challenges which necessitate educators' involvement in ensuring that children have safe, rewarding and educational web experiences. Teachers can help their students assess the value and importance of information that they find. Educators need to emphasize to students why their privacy is important and instruct them on how to avoid the traps of disclosing personal information which could be available to potential offenders. Educators can also model for students how to check the policies of web sites to be an informed surfer online and what actions to take when they become aware of a threatening incident. Ethical, safe and socially conscious online behavior may positively transform the nature of social interactions among youth and counter the betrayal, coercion and deception that accompany destructive behavior.

The Internet is a powerful environment for enhancing the transfer of social and emotional skill development. It is replete with teachable moments when young people are challenged to exhibit self-control, engage in critical decision-making, and express feelings while demonstrating respect and tolerance for others. In fact, as schools increase the amount of access students have to cyberspace, the application of social skill training to this setting will become increasingly apparent. (Berson, 2000b, p. 159)

2 The Role of Schools in Safeguarding Students Online: Case Studies

Despite the potential of technology-based learning to facilitate students' access to expansive knowledge links and broaden their exposure to diverse people and perspectives, the concomitant development of students' decision-making and problem solving skills, data processing skills, and communication capabilities has not been fully realized. Educators have often overlooked the simultaneous inclusion of technology as a topic of instruction as well as a pedagogic tool. The following two cases in the United States are indicative of emerging issues in the school setting and have initiated an evolving dialogue on the struggles of school systems to govern online activity of children and youth.

Case 1

The parents of an 11-year-old boy with a diagnosed attention-deficit hyperactivity disorder recently sued a private school in the United States for expelling their son after he visited a pornographic web site on a school computer. After being told on the school bus about a web site for "Sailor Moon" the boy sought out the site from a computer in the school's media center, expecting to get information relating to a popular fantasy cartoon. He and two friends sitting at the computer instead saw animated pornographic images with likenesses of female characters from the cartoon. Based on the child's report, he immediately logged off the web site, spending less than a minute there.

The school became aware of the incident when another student reported disruptive behavior by the three boys while they used the computer. Before the end of the school day the parents were called to a meeting with the assistant principal, who told them their son was kicked out of the \$14,000-a-year private school. The parents contend that the private school, which serves children with mild to moderate learning disorders, should have exercised more supervision over their son while he was online. Although the staff knew that the child's disorder included a tendency to engage in impulsive behavior, they allowed the child to have

open access which was indirectly monitored by faculty. Additionally, the school claimed in its catalog that it possessed a protection system with a firewall designed to protect students from reaching any Internet sites that did not fit into their curriculum.

The situation was confounded by the youth's history of prior disciplinary action by the school for inappropriate online activity after hacking into the school's computer system. Although the student had been suspended from school for his initial infraction, he subsequently retained full access to the school's technology and received no instruction or intervention to foster constructive solutions and a plan of action which fosters protective and productive learning experiences.

It should be highlighted that the school philosophy of technology use puts emphasis on the student, rather than the teacher assuming the responsibility for the daily use of the computer. The school places no requirements on the teacher to alter or use the computer as a tool in the instructional process, but rather leaves that up to the individual classroom instructional style of the teacher. Instruction in both the basic skills involved in word processing, data base management, information retrieval, and communications via email and email attachments are offered to all students in required classes at the middle school level, and for new students in the high school – at the beginning of the school year. Both elective and required computer applications classes in more advanced use of the word processing, data base management, spreadsheet, and communications software are an integral part of the school curriculum, but cyberethics and Internet safety are not formally integrated into the instructional curriculum. Moreover, younger students who have had no instruction in computer skills are provided unsupervised access to the school technology resources.

Case 2

In another case, teachers in a school district in Florida have sought liability protection from the school board for unauthorized use of the school computers by students. A collective bargaining agreement went into effect in August 2000 to protect teachers from being held responsible if students accessed inappropriate material on the Internet. The new Internet policy, which was created by a 14-member task force, stated: "A teacher shall not be liable for unauthorized use of a computer by another person unless it can be proven that a teacher did not follow school board procedures in preventing unauthorized use. All teachers are required to follow school board policy, including the acceptable use policy, which will be provided to each teacher at the start of the school year."

Procedures to prevent unauthorized use include always logging off a computer before leaving a classroom and making sure that doors to the classroom are locked so students can't access computers when the teacher is out of the room. These procedures were put in place after two incidents in which teachers were charged with allowing students to view pornographic web sites in class. In the first case, 600 pornographic sites were found on a middle school teacher's classroom computer, and the teacher was charged with displaying obscenity to a minor, a felony offense. Later the charges were dropped after an investigation revealed that the teacher rarely used the computer, and students seemed to have viewed the inappropriate sites without the teacher's consent.

In a second case the outcome was similar when charges were dropped against a high school teacher who was unaware that his classroom computer was being used by a student to view pornography when the teacher stepped out the room. These incidents reflect a national

concern over the responsibility of schools to safeguard students online and a broader recognition of the limitations of filtering software to guarantee that use will be restricted to educationally appropriate activity.

Without the bastion of Internet safety, children's vulnerability to the dark side of computer technology is exacerbated by the relative degree of on-line anonymity coupled with the lack of system-imposed restraints. School policies frequently include guidelines designed to create boundaries and barriers that promote safety when accessing Internet resources. Structuring a safe environment involves a declaration of rules, policies, and procedures that clearly communicate that the school will not support behavior that places children at risk. The Acceptable Use Policy (AUP) typically outlines expectations for behavior and consequences for infringement of the privilege to use computer resources. The signature of a child and parent denotes an understanding and acceptance of the school policies for Internet access and use. However, the posting of rules and the application of technical solutions are not sufficient outside the context of a comprehensive Internet safety plan.

3 Building Children's Defenses

Since children can be easy targets for exploitation and victimization, awareness and supervision are necessary components of any Internet safety initiative. Children may access content in cyberspace that is obscene, pornographic, violent, hateful, racist, offensive, and illegal. Consequently, the active involvement of caring adults is necessary to prepare them for safe navigation. Direct observation of children online in a public space with periodic interaction and ongoing discussions of their web experiences are the foundations of Internet safety procedures. Without this discussion, young people may be unprepared to deal with risks that they face. They may miss the warning signs or attempt ineffective solutions that can exacerbate the problem. Embarrassment and fear may prevent them from seeking assistance when problems do occur. Conversely, continual dialogue and preparation weave a net of safety.

In conjunction with early preparatory experiences which engage a child in assessing risky situations, developing appropriate coping techniques, and practicing responses to problematic situations, children can be adequately prepared for potential risks on the Internet. Avoidance techniques, de-escalation skills, and protection strategies are additional safety mechanisms children need on the Internet (Berson & Berson, in press).

Online manners (i.e., netiquette) define acceptable conduct when engaged in an interchange with people in cyberspace. They represent guidelines for relating in a courteous and respectful manner and emphasize an awareness that computers are merely the mechanism for communicating with other individuals. The application of rules which assist young people in making informed decisions and allow them to demonstrate an ability to apply online critical thinking skills facilitate productive social participation. Moreover, they counter the threat of potential disengagement of young people from positive social interactions, especially when the guidelines include limits on the time spent on the computer. Limits for children can also be set in the form of a contract and should be accompanied by open discussions about disturbing activity and content online.

Netiquette is integrally connected with global understanding, multicultural respect, diversity, and tolerance. With the advent of the World Wide Web, there is broad access to the world, but young users often lack cultural sensitivity that can foster collaboration in a global

community. Young people are especially prone to misperceive the perspectives and opinions of others and to refrain from respectful interactions. Dialogue is important for countering misconceptions and bolstering children's perceptions of themselves and others.

When the rules for appropriate conduct are combined with skills in information literacy, young people are more capable to critically evaluate information found on the Internet. The ability to discern between commercial information, advertising, propaganda, opinion and fact prepares young people for wondrous discoveries and counters potentially frightening realities in cyberspace. It is common for the technology skills of youth to surpass their critical thinking and judgment skills. While laws and attitudes struggle to keep pace with the activity online, educators, in conjunction with parents, have the opportunity to systematically attend to issues of accountability, responsibility, tolerance, and respect.

Due to the extensive interaction between school personnel and students during the instructional day, educators have an important opportunity to observe children, establish a reasonable level of suspicion, and intervene for the protection of children and the support of families. Yet, school staff notes a general lack of knowledge of Internet safety and cyberethics. Educators in this process may play an integral role; however, they tend to lack confidence in their range of knowledge of technology and their ability to provide appropriate prevention information to children and their families. Consequently, as society struggles to address the serious social and public health problem of Internet use, educators often find themselves inadequately prepared to assist children in the classroom. A lack of adequate knowledge has been identified as a significant barrier to detecting and intervening on behalf of children. Teachers typically do not feel equipped to address their evolving role in safeguarding the emotional and physical well being of children. A general lack of knowledge of online safety combined with an overburdened staff means that many cases of cyberabuse are overlooked. Detection can be complicated by competing priorities of an intense work schedule in the schools with crowded classrooms. Teachers may have little time to engage in intensive reflective observation of individuals in the schools and lack skills in discriminating between serious infractions. Even more pervasive is a lack of understanding of how to respond when the impact of cyberactivity affects the educational and socio-emotional development of the child.

These observations note the importance of the interplay between legal mandates, personal experience, and institutional response, and demonstrate the need to involve educators in training and collaborative initiatives. Of special concern to educators should be the creation of prevention programs which are focused on children with developmental disabilities and emotional and behavioral disorders. Specific training in the University and inservice professional development should highlight the potential for inappropriate use among high-risk populations of children.

Schools cannot address issues of technology use and misabuse in isolation. Interagency collaboration and the pooling of resources are critical. Even among the more progressive districts where Internet safety has been integrated into instruction, prevention programs for parents and educators are less common. Principals and community agencies report that child-oriented prevention programs are not integrated into school policy, and standardized programming is not structured by the district for all children to access. This piecemeal approach to prevention lacks the critical parent and community program components which are necessary for full implementation. Establishing a collaborative endeavor between multidisciplinary groups and education programs may bridge the rift between teacher training

and practice standards which meet the needs of children for safe and productive online learning.

4 Concluding Thoughts

The positive potential of empowered interaction can be lost when constructive behaviors are replaced with offensive and harmful acts. Part of the process of safeguarding children's experience online is the active instruction to educate children to navigate safely in cyberspace. Some educators and caregivers will abdicate their responsibility for action to technological solutions which filter, monitor, and guide our youth through the complex world of cyberspace. However, a human touch is needed to counter the dark side of the Internet where sexual and racial harassment, obscenity, hate, and violence converge with caring and respect (Willard, 2000). This involves more than disseminating practical lists of online safety tips and requires a comprehensive educational program, which is part of a dynamic and interactive experience involving teachers, parents and youth in the development and training process. Educational strategies which focus on helping children and youth to develop autonomous and responsible skills online require education. This approach complements existing filters and security systems which can never guarantee total protection. Initiatives which mediate online experiences that are disadvantageous to a child's physical, cognitive, and socio-emotional functioning should be developed in conjunction with early preparatory experiences which engage youth in assessing risky situations, developing appropriate coping techniques, and practicing responses to problematic situations. Young people can be adequately prepared for potential risks on the Internet by learning how to identify ambiguous situations, take appropriate steps to minimize their vulnerability and augment their abilities to make informed decisions for safe navigation online. Avoidance techniques, de-escalation skills, netiquette/ethics training, and protection strategies are among the critical safety mechanisms which should be infused into instruction. The educational process can promote safer use of the Internet through competencies and attitudes targeted toward children in cyberspace.

References

- Berson, I. R., Berson, M. J., & Ferron, J. (in press). Emerging risks of violence in the digital age: Lessons for educators from an online study of adolescent girls in the United States. *Journal of School Violence*.
- Berson, M. J. (2000a). The computer can't see you blush. *Kappa Delta Pi Record*, 36(4), 158-162.
- Berson, M. J. (2000b). Rethinking research and pedagogy in the social studies: The creation of caring connections through technology and advocacy. *Theory & Research in Social Education*, 28, 121-131.
- Berson, M. J., & Berson, I. R. (in press). Internet safety. In A. Kovalchick & K. Dawson (Eds.), *Encyclopedia of Educational Technology*. Santa Barbara, CA: ABC-CLIO.
- Cole, J. I., et al. (2001). *UCLA Internet Report 2001: Surveying the Digital Future Year Two*. Los Angeles, CA: UCLA Center for Communication Policy. Available at www.ccp.ucla.edu

Willard, N. (2000). *Choosing not to go down the not so good cyberstreets*. Paper presented to the National Academy of Sciences Committee on the Study of Tools and Strategies for Protecting Kids from Pornography and their Applicability to other Inappropriate Internet Content. Washington, DC.

Young, K. S. (1998). *Caught in the net: How to recognize the signs of Internet addiction and a winning strategy for recovery*. New York: John Wiley & Sons, Inc.

Acknowledgements

The ongoing investigation of children's activity in cyberspace, including implications for education professionals, was partially supported by the University of South Florida Collaborative for Children, Families, and Communities, the University of South Florida PT3 Grant, the Juvenile Welfare Board of Pinellas County, the University of Virginia's (UVA) Curry Center for Technology and Teacher Education PT3 Catalyst Grant, and the UVA IMPACT II Project.

Michael J. Berson is an Associate Professor of Social Science Education in the Department of Secondary Education at the University of South Florida. He is a member of the United Nation's Education, Scientific, and Cultural Organization (UNESCO) North American Child Health Task Force Advisory Committee on Internet Safety. Michael's research explores technology in social studies education and global child advocacy. He can be contacted at berson@tempest.coedu.usf.edu