

# National Cyber Security Alliance

## **A Need for Comprehensive Cyber Ethics, Safety and Security Education within the United States**

### Executive Summary

**Technology Literacy has recently gained attention as the No Child Left Behind (NCLB) requirement states** “student academic achievement [will be improved] through the use of technology in elementary schools and secondary schools through assist[ing] every student in crossing the digital divide by ensuring that every student is technologically literate by the time the student finishes the eighth grade, regardless of the student's race, ethnicity, gender, family income, geographic location, or disability” (NCLB, 2001). **The mandate to have all students technologically literate by the eighth grade has caused states to quickly implement plans that will help students reach these goals.** The National Educational Technology Standards (NETS) for Teachers, Administrators and Students helps provide a framework to guide educational leaders in recognizing and addressing the essential conditions for effective use of technology to support K-12 education.

Numerous national and state initiatives that target technology literacy education seek to expand the ability of our students to use technology both to enhance their education and to prepare for future careers, as computers and technology are a cornerstone of 21<sup>st</sup> Century Skills. However, while the use of technology is growing, there is not always a commensurate increase in awareness of the most ethical, safe and secure practices when using technology.

Current media has focused on Internet safety issues, prompting increased activity related to social networking sites and chat rooms. Indeed, the public is increasingly concerned with finding ways to help protect children while they are on the Internet. According to a recent University of Michigan National Poll on Children’s Health Issues (May, 2007<sup>1</sup>), adults ranked “Internet Safety” as the seventh most important issue affecting children.

This increased public interest has caused lawmakers, education leaders and the Internet industry to look for new ways to help protect children from contact with predators and inappropriate material in chat rooms and on social networking sites. In some cases, states and lawmakers have focused on drafting legislation that requires age verification, calls for increased law enforcement and even new regulation. But safety is just one area among the larger complex landscape of issues related to cyber awareness.

While policymakers have sought legislative solutions to help protect children online, potentially more effective and under explored ways to ensure children don't become victims of cyber crime are: (1) making sure every school and library in the country teaches our children at least a minimum set of prevention methods in all areas of cyber awareness necessary to help them recognize, respond to and report potentially dangerous situations they may encounter online, and (2) equipping our teacher workforce with the knowledge to help them recognize and react to potentially dangerous situations, and work in such a way that they are modeling proper and safe behavior to their students.

In the past, schools and libraries have led the charge to educate our youth on ways to protect

<sup>1</sup> <http://www.med.umich.edu/mott/research/chealthconcernpoll.html>

themselves from threats they may come across in their neighborhoods, like “don’t talk to strangers” or “don’t drink and drive.” These prevention classes have worked, and proven successful in teaching students methods of staying safe in the real world. However, students are receiving mixed messages with regards to online behavior as the push for Internet literacy and integration in the classroom increases, sometimes without appropriate support for the teaching of safer and more secure online habits and practices. Moreover, the current lack of awareness and education of parents and home-users further complicate the issue.

The lack of coordinated leadership on the national and state level to integrate cyber prevention lessons within an academic setting on a systemic level is cause for concern. Some schools and libraries are doing their best to fill that leadership void with very little guidance or support. This approach has resulted in *ad hoc* cyber-safety lessons that are irregular and may only focus on one subject area -- such as cyber predators -- rather than classes that cover the whole online-threat landscape. Oftentimes, even this limited cyber-safety education fails to exist.

To ensure children receive a thorough cyber-safety education to help them avoid the multitude of threats they may face online, cyber-awareness prevention programs must incorporate ***cyber ethics, cyber safety and cyber security (C3)*** principles (Pruitt-Mentle, 2000). Not doing so could lull students into a false sense of confidence by only focusing their attention on one online threat such as cyber predators, when there are many others that exist today, and other risks that have yet to emerge.

To help address this need, the National Cyber Security Alliance stepped forward to lead a team of government agencies, education groups and Internet companies. Our purpose is to draft a framework that states can use as a road map to help develop a comprehensive approach to implementing C3<sup>TM2</sup> lessons within schools, libraries and after-school programs.

This framework is based on successful curriculum models that look to states’ departments of education to lead individual statewide efforts. Each state can develop guidelines providing local school districts with the flexibility to integrate C3 curricula and programs in ways that best address local needs. Schools and libraries should be given the freedom and flexibility to find ways to incorporate C3 curricula within already existing prevention programs and lessons. The framework emphasizes the need for all three critical components: cyber ethics, safety and security, and should be systemic in delivery and seamlessly taught throughout the K-12 experience as both educator and administrator professional development and lessons.

## **Background**

### ***Public Concern Over Children Staying Safe Online***

Recently, cyber security and safety for children has become a top concern among parents and the public at large. The National Poll on Children’s Health Issues (2007) asked adults to rate 17 different health concerns that directly affected their children on a daily basis. For the first time since the poll was conducted, “Internet safety” was among the top 10 concerns, and was rated as the seventh most important child health issue. Internet safety ranked higher than “School Violence (8),” “Sexually Transmitted Infections (9)” and “Abuse and Neglect (10).”

In addition, the National Cyber Security Alliance (NCSA) recently conducted focus groups with adults ranging from 18 to 65, and found that the majority of adults assumed schools are already teaching cyber ethics, safety and security classes. Most of them felt that if schools were not currently teaching

<sup>2</sup> C3 is a trademark of Educational Technology Policy, Research, and Outreach, Inc. and is used with its permission

such classes as part of their curricula, they should be. According to the focus group participants, parents feel overwhelmed with the task of teaching their children the technical aspects of how to protect their identities and information online, and look to educators as the best suited to provide such training and encourage safe habits and practices. Parents often lack the knowledge themselves and sometimes do not own or utilize a computer in their own working environments.

Based on NCSA's research, there is a clear expectation among adults, parents and constituents that school districts and their education systems are already or should be integrating cyber security, safety and ethics lessons into the class curriculum. However, the types of cyber-prevention lessons that are actually being taught in schools, libraries and after-school programs may not live up to the public's perception and expectations. Additionally, either there are no computers at home, or parents fail to reinforce these lessons by words or actions. Indeed, for many in our population, the educational setting is the only location with both the tools and the information needed to fill this critical void.

### ***Threats Children May Face While Online***

Recent media attention may leave many Americans with the impression that the only threats children face while online are from pedophiles and cyber predators. This assumption is wrong. While protecting children from cyber predators is an incredibly important issue and should be regularly addressed, cyber predator or safety issues account for only one portion of the threats students could face while on the Internet.

It is also important to recognize that youth-risk online must be viewed from the perspective of adolescent risk. Many young people simply require better insight into what they can and should do to help keep themselves safer and more secure. Other youth are more at risk of engaging in threatening or irresponsible offline behavior.

A more comprehensive list of the cyber threats that children could face while online follows....

### ***Cyber Safety - Sexual Solicitation/Child Predators/Other Sexual Risks***

Unfortunately, there is a chance that children could receive a sexual solicitation while on the Internet, or communicate with an adult who wants to meet a child offline with the intention of harming the child. According to a recent National Center for Missing and Exploited Children and University of New Hampshire Study, one out of seven children received a sexual solicitation while on the Internet. Due to the amount of media coverage this potential threat has received over the past two years, most adults are aware of these types of cyber-safety threats.

However, a closer analysis of this study will reveal that the situations that were considered to constitute sexual solicitation included "situations where someone on the Internet attempted to get them to talk about sex when they did not want to or asked them unwanted sexual questions about themselves." (p 15). It is also important to understand that 43% of those solicitations came from individuals who were known or perceived to be other teens (p. 17) and "most youth (66%) were not particularly upset or frightened by the solicitations" (p.20). Additional research into the potential dangers of online solicitations is needed, particularly to support identifying the most effective means of addressing the population of young people who are engaging in online sexual solicitation or other risky sexual behaviors.

Further, the Crimes Against Children Research Center report (2007) revealed that 34% of youth

experienced unwanted exposure to online sexual material, despite an increase in content filtering. In many situations this exposure likely could have been prevented and limited in scope through effective education into protection and response strategies.

### ***Cyber Security - Identity Theft/Internet Fraud***

In our information-centric world, children are assigned social security numbers at birth and are often given credit cards and cell phones when they are teenagers. These numbers are extremely valuable to criminals, and young people are easier targets than more sophisticated adults. As a result, students are increasingly becoming victims of identity theft and fraud. It is entirely possible that students could become victims of identity theft before they even graduate from college or reach the age of 23. According to the Federal Trade Commission (2007), 5% of all identity theft victims in 2006 were under the age of 18. Moreover, 18 to 29 year olds comprised the largest percentage of identity theft victims in 2006. Increasing numbers of high school and college age students are falling victim to identity theft, and it is important that students of all ages be made aware of the dangers associated with identity theft and fraud on the Internet.

### ***Cyber Ethics - Cyber Bullying***

Additionally, students are increasingly faced with cyber bullying -- the electronic equivalent of playground harassment -- as bullies move from the schoolyard to the Internet. According to a 2006 National Center for Missing and Exploited Children and University of New Hampshire study, online harassment rose more than 50% between 2000 and 2006, and 44 % of those harassing communications came from the victims' peers. In addition, "one-third of all teens using the Internet have been the victims of cyber-bullying," according to a study by the Pew Internet & American Life Project. Thirty-eight percent of girls reported being bullied online, compared with 26 percent of boys. Also, nearly four in 10 users of social-networking sites said they have been cyber-bullied in some way, compared with 22 % of those who do not use such sites.

Other concerns regarding Internet ethical, safety and security use include:

- Unsafe online communities – online communities that support engagement in harmful behaviors as self-cutting, anorexia, drug use and suicide
- Hate groups and gangs
- Gambling and gambling-like activities
- Hacking and other computer security crimes, and
- Copyright infringement and plagiarism.

### ***Importance of Understanding The Complete Internet Landscape***

Policymakers, educators and parents need to be aware of the range of cyber ethics, safety and security issues children may face online. Understanding the full Internet landscape will help the public better recognize the need to teach children appropriate ***cyber ethics, cyber safety and cyber security, (C3) principles***. By using C3 principles in all cyber-related lessons and programs, children will become

familiar with more of the tools necessary to avoid becoming a victim of cyber crime and they will be empowered to become better cyber citizens as they mature.

## **What Is The Current State Of Cyber Ethics, Safety and Security Education in the United States?**

While there is no formal research that quantifies how many schools, libraries and after-school programs have integrated C3 lessons within already existing curricula, there are very few states requiring cyber-awareness lessons and programs. Even fewer states are taking a statewide approach to ensuring schools, libraries and after-school programs have the resources, know-how and means to teach C3 lessons.

Currently, the State of Virginia is the only state with a law in place requiring schools to teach Internet safety and security lessons on an annual basis. While we applaud Virginia's first steps, we note that even this effort does not cover all the C3 principles, as it does not include ethical issues. California and New York have legislation pending to require schools to teach online safety, while other states are looking for ways to include such lessons in their statewide "technology in the classroom" mandates.

*Ad hoc* programs or lessons are incorporated in many states' education systems, but these programs are most likely only geared toward teaching kids how to avoid cyber predators and do not include sustained and comprehensive C3 lessons and curricula that address other important issues. Even more concerning, teachers are not always provided with training that would allow them to gain additional knowledge and skills; they are simply given a lesson to teach. Without accompanying instruction grounded in a systemic approach to C3 and the means to gather additional information, the lessons become a single unit that is not integrated into day-to-day classroom activities and home behaviors.

## **Cyber Ethics, Safety and Security Principles/Lessons**

Children face a wide range of threats on the Internet beyond just cyber predators and cyber safety. By not teaching children methods and practices to recognize, respond to and report the threats they may face on the Internet, children could perceive that the only preventative measures they need to take while online are to avoid cyber predators. This could lull them into a false sense of security, and make them an easier target for identity thieves, phishers, pharmers and other cyber criminals. As a result, the NCSA stands united behind the notion that students should be regularly taught preventative lessons based on the C3 principles within schools, libraries and after-school programs. More specifically, the C3 principles are defined as:

- A. **Cyber Ethics Lessons**: Children are taught from an early age that stealing something from someone's desk or breaking into someone's home is wrong and against the law, but sometimes forget that these same ethics apply in the cyber world. For example, hacking into someone's computer and taking information is just as wrong – and illegal -- as breaking into someone's home. Intellectual property laws are being ignored as plagiarism and file-sharing via the computer are easier, yet just as wrong as plagiarizing a hardcopy text or stealing a music CD from the store. Cyber bullying is just as wrong as bullying someone on the playground. Rules and codes of acceptable conduct must be set in the virtual world, just as they are in the real world. By working to instill these values, children can be better prepared to be responsible,

ethical consumers of technology.

- B. **Cyber Safety Lessons:** These lessons should incorporate many social behavior tips to help protect children from online dangers, such as ways to avoid cyber predators, harassment, unwanted communications and cyber bullies. In addition, children need to be able to recognize a potentially dangerous online situation and respond appropriately, including when and how they might report online threats. Lessons also need to address important foundational aspects of online safety, including knowing how to best safeguard personal safety during various online activities; effectively assessing the credibility of online information, and acquiring strategies for interacting with online strangers. There are a number of ways in which children's personal information can be compromised: e.g., information posted to wikis and blogs, and stored on cell phones and laptops. Students and teachers must be instructed regarding the host of dangers and mitigation strategies for these environments.
  
- C. **Cyber Security Lessons:** In addition to teaching a child about how to turn on a computer, type in a URL and use a mouse, online security includes teaching children how to be more computer-savvy and secure. Information regarding ways students can help secure their computers, identities and financial information are very important so children understand how to protect their identities throughout their lives. Recognizing the need for strong passwords, effects of viruses, characteristics of spam, and the dangers of responding to phishing and pharming schemes, is imperative. Students need to understand the negative consequences that might occur, both to their personal computers and information and to our society and economy as a whole.

### **A Framework for Implementing State-Wide Cyber Ethics, Safety, and Security Lessons and Programs within Schools, Libraries and After-School Programs**

The proposed outline below suggests that states should use the C3 framework as a starting point to gather the appropriate stakeholders with expertise within the topic area, and provide them with a road map on key aspects that should be included in any program or curricula. At a minimum, all of the following principles should be incorporated in any final approach that seeks to teach children how to best stay safe online.

**A State's Department of Education should create a working group made up of state and local education leaders, school safety personnel, and officials from the mental health, consumer protection, technology and law enforcement arenas, to collaborate and develop flexible guidelines that assist local school districts in incorporating cyber ethics, safety and security curricula into the classroom.**

**Explanation:** To ensure educators have access to creditable and effective lessons on key cyber ethics, safety and security topics, a State's Department of Education should develop a Cyber Ethics, Safety and Security Working Group that includes state and local leaders from the education community, education technology personnel, school safety personnel and officials from the mental health, consumer protection, technology and law enforcement arenas. This C3 working group will then be charged with developing guidelines to assist local school districts in creating ways to incorporate C3 lessons into

classroom activities. The advantage for the Department of Education in developing a C3 Working Group is that it can leverage the expertise of different organizations, government agencies and educators to suggest the most effective and up-to-date methods for teaching C3 lessons, while at the same time making sure the guidelines are developed in a way that allows for flexibility and customization within a given school district. Moreover, the working group can be used to find credible materials that can be made available to educators. The Departments of Education have experience in building coalitions to address youth safety and technology concerns through the No Child Left Behind Act, including the Enhancing Education through Technology (Title II-D) and the Safe and Drug Free Schools and Communities (Title IV-A). Programs

**Any effort to implement statewide cyber-awareness lessons or curriculum in public schools and libraries must include cyber ethics, safety and security lesson topics.**

**Explanation:** Although some school districts and states have started to implement cyber-safety lessons, or lesson plans, those efforts might not include cyber security and ethics curriculum. Cyber safety curriculum only accounts for one third of the cyber awareness needs that all students should be knowledgeable about in today's cyber society. As a result, any statewide cyber-safety curriculum or school program must include cyber security, cyber safety and cyber ethics (C3) topics in the curricula. This will help prepare students for dealing with the range of threats they may face online, so they can become responsible cyber citizens in the future. Otherwise, students and adults are more likely to continue to fall victim to cyber fraud, harassment and an array of other flavors of cyber crime.

**Individual localities should have the flexibility to determine the method or manner in which C3 curriculum or instruction is administered.**

**Explanation:** While it is incredibly important to ensure cyber ethics, safety and security are taught, different schools and libraries may have different styles and methods for delivering lessons on these topics. It is important to give schools and libraries an opportunity to choose from the array of cyber ethics, safety and security curriculum available to them, so they can find material best suited to their needs. Not giving schools and libraries the flexibility to update and choose their curriculum could have negative unintended consequences, such as using out-of-date materials. As we all know, cyber crime moves at Internet speed, is ever-changing and presents us with new challenges daily. Schools and libraries need the flexibility to deal with these new challenges and to provide students with the most recent materials and methods to help address cyber threats.

**State and local support should be provided to fully implement Cyber Ethics, Safety and Security programs.**

**Explanation:** Most parents and educators will agree that teaching cyber ethics, safety and security to students is incredibly important in this information age. At the same time, states and localities have limited funding to institute and manage a number of initiatives, including incorporating C3 lessons and curriculum. Understanding this is a national problem and that most constituents would support schools and libraries that provide lessons or curriculum that teach students how best to stay safe online, the federal government should provide resources, where available, to help state and local school districts implement and incorporate C3 curriculum. Meanwhile, educators may want to seek out C3 resources that

are readily available on the Internet and made available at no charge through non-profit organizations. Without proper funding, new programs strain local school district resources and have a high probability of never being integrated. Teaching C3 lessons sporadically will only diminish their effectiveness. Thus, such programs must be implemented and supported with adequate, ongoing federal funding.

**Professional development opportunities for staff across the division should be given when incorporating cyber ethics, safety and security curricula in school districts.**

**Explanation:** If educators are to teach children how to best stay safe online, teachers must understand the material they teach. They must know firsthand how to use the technology their students use, and they must fully understand how to avoid dangers on the Internet and through other electronic communications. Since students pick up technology very quickly and may understand some technological concepts before learning them in the classroom, it is important that educators “keep up” with their students. Therefore, educators must be given professional development opportunities to both understand and teach specialized C3 curricula.

**States, schools and libraries should develop an evaluation component that regularly examines their cyber ethics, safety and security programs’ effectiveness and recommend revisions.**

**Explanation:** States, schools and libraries should regularly evaluate their C3 program to see whether it is the best method to teach key C3 principles, and whether the chosen course materials are effective. Moreover, with the constant evolution of cyber crime and technology, educators may want to find new materials and focus their lessons on new technologies and the potential issues they present. For instance, social-networking websites are a fairly new phenomenon and have become extremely popular over the past four years. These services present new risks and challenges that students may not have envisioned previously. Under the Safe and Drug Free Schools and Communities Act, schools are required to implement research-proven best practices Section 4115 (a)(1). It will not be possible to address Internet safety, security, and ethics concerns using research-proven best practices because the risks are new, research insight is limited, and new concerns are emerging with each new technological development. The standards set forth in Section 4115 (a)(3) that provide the requirements necessary to request a waiver from the Principles of Effectiveness should be incorporated into the C3 programs.

**Cyber Ethics, Safety and Security education programs for parents should be made readily available within local school and library districts.**

**Explanation:** The best way to ensure students practice the C3 lessons or curriculum taught in schools or libraries is to have their parents reinforce and practice the same ethics, safety and security principles. No matter what students or teenagers say, they learn by example and mimic what their parents do and how they act. If parents don’t make cyber ethics, safety and security a priority nor incorporate proper cyber-security practices into their daily routines, neither will their children.

Parents may want to make cyber ethics, safety and security a priority, but might not have the technical skills or knowledge to do so. Furthermore, Internet safety programs recommend to children and teens that they report online concerns to adults. Young people are unlikely to report problems to parents if they do not perceive that their parents will understand how to effectively address the concern.

There is a clear need to provide parents with the opportunity via programs on a local level to help them understand how the Internet works, the latest threats their children may face and the various parental control tools and technology available. One way to provide parents with such a service is for communities to partner with their schools and libraries to deliver and hold cyber security and safety “town halls” or workshops. Schools and libraries provide a great central location for ongoing C3 education for parents, and typically have local Parent Teacher Associations that can assist in promoting and launching such programs. It is critical that parents have the knowledge and resources to enable them to exercise appropriate C3 practices. With parental support and reinforcement, it is more likely that children will have the expertise to stay safer and more secure online and become stand-up cyber citizens in the future.

### **About the National Cyber Security Alliance**

The National Cyber Security Alliance (NCSA) is a not-for-profit 501(c)(3) organization and a go-to resource for cyber security awareness and education for home user, small business, and education audiences. A public-private partnership, NCSA sponsors include the Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organizations. NCSA provides tools and resources to empower home users, small businesses, and schools, colleges, and universities to stay safe online.

In particular, the NCSA works with the K-12 community to provide educators and administrators with resources that will help them provide students with cyber ethics, safety and security lessons and curricula. Ensuring students receive the proper cyber security, safety and ethics instruction will help them become better cyber citizens. This objective fulfills the NCSA’s mission to foster a more cyber savvy and secure public.

### **National Cyber Security Alliance's partners that support/and or participated in the development and/or review of this white paper:**

- Business Software Alliance
- C3 Institute
- CA
- Center For Safe and Responsible Internet Use
- ConnectSafety.org
- The Consortium for School Networking
- CyberSmart!
- Educational Technology Policy, Research and Outreach, University of Maryland, College of Education
- Enough is Enough
- iKeepSafe Coalition
- Institute for Infrastructure and Information Assurance at James Madison University
- International Society For Technology in Education
- (ISC)2
- McAfee
- Microsoft
- NetFamilyNews.org
- RSA, The Security Division of EMC

- Safe Surfin' Foundation
- SafeKids.org
- Software and Information Industry Association
- State Educational Technology Directors Association
- Symantec