



**StaySafeOnline.org**  
National Cyber Security Alliance

Media Contacts:

Aimee Larsen Kirkpatrick  
National Cyber Security Alliance  
202-570-7431  
[aimee@staysafeonline.org](mailto:aimee@staysafeonline.org)

Katherine Hallen  
463 Communications  
202-463-0013 x213  
[katie.hallen@463.com](mailto:katie.hallen@463.com)

Christine Aguirre  
Microsoft  
425-761-4514  
[caguirre@microsoft.com](mailto:caguirre@microsoft.com)

## **2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey**

*America's K-12 schools not preparing kids for digital age, study finds.*

**WASHINGTON — May 4, 2011** — A study released today from the National Cyber Security Alliance (NCSA), sponsored by Microsoft Corp., finds that schools are ill-prepared to teach students the basics of online safety, security and ethics — skills that are necessary in today's digital times. At the surface, America's K-12 schools embrace the digital age, with dedicated computer labs, technology-integrated classrooms and students well-versed in the Internet as a means for homework and a social life. That said, administrators, teachers and IT coordinators do not agree on the best approach to ensure children are prepared for the digital age.

The 2011 edition of **State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey**, previously published by NCSA in 2008 and 2010, found contention among school leaders regarding whether online safety, security and ethics should even be taught as part of a district curriculum. Only 55 percent of teachers strongly agree that cybersecurity, cybersafety and cyberethics should be taught in schools as part of the curriculum, while more than 82 percent of administrators and 85 percent of IT specialists share those same strong feelings.

Further pointing to a disconnect, 51 percent of teachers agree their school districts do an adequate job of preparing students for online safety, security and ethics, while 81 percent of administrators and 81 percent of IT coordinators believe their districts are doing an adequate job.

“Kids and teens have embraced the digital world with great intensity, spending as many as eight hours a day online<sup>1</sup> by some estimates,” said Michael Kaiser, executive director of the NCSA. “Yet America's schools have not caught up with the realities of the modern economy. Teachers are not getting adequate training in online safety topics, and schools have yet to adopt a comprehensive approach to online safety, security and ethics as part of a primary education. In the 21st Century, these topics are as important as reading, writing and math.”

### **Teachers Don't Receive Professional Development**

The study found that more than one-third of teachers (36 percent) received zero hours of professional development training by their school districts in issues related to online safety,

security and ethics in the past year. All told, 86 percent received less than six hours of related training.

Not surprisingly, teachers don't feel well-prepared to teach these topics. Only 24 percent feel very well-prepared to teach about protecting personal information online; 23 percent feel well-prepared to teach about the risks of cyberbullying; and one-third feel well-prepared to teach basic computer security skills, such as password protection and backing up data.

“Schools have a responsibility to prepare kids to be smart, capable and thoughtful digital citizens,” said Jacqueline Beauchere, a director in Microsoft’s Trustworthy Computing Group. “It’s a matter of local and global importance. Not only must students know how to stay safer online at school and at home, but they also must be equipped to deal with the workplace challenges of the digital age. Teachers will need training and support to ensure that they have the skills and confidence to cover these topics in the classroom.”

### **Few Teachers Addressed Hate Speech, Cyberbullying**

Despite constant news coverage over the past 12 months, only 15 percent of teachers taught students about hate speech, and 18 percent taught students how to deal with alarming posts, videos or other Web content. Just 26 percent taught kids how to handle incidents of cyberbullying.

One-third of teachers covered risks tied to social networking sites, and another third taught students about sharing personal information on the Internet. However, schools are slow to respond to emerging challenges in safety and security. Just 6 percent taught students about the safe use of geolocation services, despite the rise in the use of Web-enabled mobile devices.

### **Graduating Cybersecurity-Capable Students: Shared But Unmet Vision**

The study found that 97 percent of administrators agree schools should have curriculum throughout K–12 that prepares young people to enter the workforce as cybercapable employees — meaning they are able to use basic technology in a safer and more secure way. Overall, 68 percent of administrators believe their schools or school districts are doing an adequate job of preparing students to pursue college-level education in cybersecurity.

Yet, few K–12 educators are teaching topics that would prepare students to be cybercapable employees or cybersecurity-aware college students. In the past 12 months, 20 percent taught about knowing when it is safe to download files; 23 percent taught about using strong passwords; and just 7 percent taught about the role of the Internet in the U.S. economy. Disappointingly, a mere 4 percent taught about careers in cybersecurity.

“The survey reveals a critical need for new curricula and teacher training that will encourage safe, secure and responsible behavior among school students,” said Dena Haritos Tsamitis, director of Carnegie Mellon University’s Information Networking Institute, as well as director of education, training and outreach at the university’s CyLab. “It’s essential to address this need in order to prepare a cybersavvy workforce for our nation’s future.”

The study points to lingering questions about who bears the primary responsibility for teaching kids about digital safety, security and ethics — parents, teachers or government? Nearly 80 percent of teachers and 60 percent of administrators identified parents as primarily responsible for teaching children to use computers safely and securely. However, more than half of IT coordinators said teachers bear the primary responsibility. Across all groups surveyed, less than 1 percent indicated government or law enforcement shouldered the main responsibility.

### **Online Safety: A Shared Responsibility, a National Priority**

The NCSA advocates for a comprehensive approach to teaching online safety, security and ethics to be part of K–12 education nationwide. Given the level of confusion school leaders seem to have — from the best approach to teaching these subjects down to who bears the primary responsibility for a child’s education — it’s never been more important that school districts clarify responsibilities and identify a clear course of action.

“Every school district should have a comprehensive cybersecurity curriculum in place. Schools should be confident that they are graduating students who can use technology safely, securely and productively, and this training should begin at an early age, from the point when a child first enters school,” Kaiser said. “Teachers, administrators and other school personnel must be supported as we evolve to teach the basics of a cybersecurity education to every child. Teachers need training, and schools need high-quality curricula that address the needs of students who are growing up in digital times.”

Kaiser continued: “Just as we would not hand a child a set of car keys with no instruction about how to drive, we should not be sending students out into the world without a solid understanding of how to be safe and secure online. It’s critical to our economic and national security, and it’s our shared responsibility as parents, educators and citizens.”

For the 2011 study, Zogby/463 surveyed 1,012 teachers, 200 IT coordinators and 402 school administrators (325 principals and 77 superintendents) in January and February, via online surveys and telephone interviews. Teachers had a margin of error of +/- 3.1 percentage points, IT specialists of +/- 7.1 percentage points and school administrators +/- 5.0 percentage points.

More information about the 2011 State of K–12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey is available:

[\\*Download full report with study findings](#)

[\\*Download fact sheet](#)

[\\*View the “2011 State of Cyber Education Infographic”](#)

### **About The National Cyber Security Alliance**

The National Cyber Security Alliance is a non-profit organization. Through collaboration with the government, corporate, non-profit and academic sectors, the mission of the NCSA is to

empower a digital citizenry to use the Internet securely and safely protecting themselves and the technology they use and the digital assets we all share. NCSA works to create a culture of cyber security and safety through education and awareness activities. NCSA board members include: ADP, AT&T, EMC Corporation, Cisco Systems, Facebook, General Dynamics Advanced Information Systems, Google, Lockheed Martin Information Systems & Global Services, McAfee, Microsoft, PayPal, Science Applications International Corporation (SAIC), Symantec, Verizon and Visa. Visit [www.staysafeonline.org](http://www.staysafeonline.org) for more information.

## **About Microsoft**

Founded in 1975, Microsoft (Nasdaq “MSFT”) is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

<sup>1</sup> A 2010 Kaiser Family Foundation study found that 8- to 18-year-olds devote an average of seven hours and 38 minutes to using entertainment media across a typical day (<http://www.kff.org/entmedia/entmedia012010nr.cfm>).

### **For more information, press only:**

Rapid Response Team, Waggener Edstrom Worldwide, (503) 443-7070,  
[rrt@waggeneredstrom.com](mailto:rrt@waggeneredstrom.com)

*Note to editors:* For more information, news and perspectives from Microsoft, please visit the Microsoft News Center at <http://www.microsoft.com/news>. Web links, telephone numbers and titles were correct at time of publication, but may have changed. For additional assistance, journalists and analysts may contact Microsoft’s Rapid Response Team or other appropriate contacts listed at <http://www.microsoft.com/news/contactpr.msp>.