

# Trustworthy Computing

## Microsoft and Mandatory Online Safety Education

September 2009

### ***Introduction***

Governments around the world are investing in educational technology and related curricula. Yet very few governments *require* public schools to teach comprehensive Internet safety curriculum, even though safety experts identify education as the most effective means of protecting children from online risks. In the United States, five states have currently mandated online safety education and several more are building similar programs. Promising efforts have also begun in countries as diverse as Egypt, Romania and Ireland, but to date we know of no other comprehensive online safety education programs. To address this lack of consistency, Microsoft supports mandatory Internet safety education as part of school curriculum.

We believe Internet safety curricula should become an integral part of school systems' efforts to achieve technological literacy for their students, and should include three basic elements:

- **Cyber Safety:** How to recognize and avoid inappropriate solicitation, child predators, bullying and other risks;
- **Cyber Security:** How to recognize and avoid identity theft and Internet fraud and to protect computers from viruses and other threats;
- **Cyber Ethics:** How to be a responsible cyber citizen.

### ***Background: An Urgent Need***

In a U.S. poll on Children's Health Issues conducted by the University of Michigan (2007), adults ranked "Internet Safety" as a top concern, giving it a higher priority than "School Violence," "Sexually Transmitted Infections," and "Abuse and Neglect." Many parents view online safety as a central element of the curriculum, comparable to basic health education, driver's education and crime prevention. In fact, most people believe that their schools already teach basic Internet safety practices. Unfortunately, few schools do, and others do so incompletely.

U.S. federal legislation, the 2002 "No Child Left Behind Act", requires that all students achieve technological literacy before they finish the eighth grade. Microsoft believes that curriculum should cover online safety, security and ethics and should extend from grades K-12. State Departments of Education should propose model curriculum and provide technical assistance. A number of resources are available for free, including programs from NetSmartz, Look Both Ways, WebWiseKids, Wired Safety/TeenAngels, and the i-SAFE "iLearn" online modules that Microsoft helped develop.

### ***Knowing the Risks and How to Avoid Them***

*Cyber Safety:* For all its opportunities to learn, play, and connect, the Internet also brings a variety of risks. Many people—including children—are aware that some sexual predators use the Internet to target children. But it's important to identify the other risks—often created or enabled by children themselves. A 2009 survey of European teenagers, sponsored by MSN, found that 29 percent had been bullied online, but the vast majority had never reported online bullying. Children and teens may also encounter online communities that encourage inappropriate behavior such as drug use, gambling, eating disorders, or even suicide.

Despite their knowledge of online risks, only 51 percent of European teens said they regularly use privacy settings to restrict access to personal information. Children should understand how their reputation could suffer from information that they—or others—post online. Embarrassing photos, videos or messages can live indefinitely online, perhaps complicating future relationships, or limiting opportunities for jobs and higher education.

- *Children should be taught basic online safety habits and ways to avoid potential dangers. They need to know how and when to report problems or issues to the appropriate adult authorities.*

*Cyber Security:* Criminals are increasingly targeting teenagers with identity theft and financial fraud schemes, since many teens now use credit cards and mobile phones. According to the U.S. Federal Trade Commission, 5 percent of identity theft victims in 2006 were under the age of 18, and 18- to 29-year-olds were the group most likely to become victims.

- *Children should learn to protect their identity and financial information online. They need to understand the need for strong passwords and learn how to update their computers and devices to protect them from viruses, spam and phishing scams.*

*Cyber Ethics:* In the European study, 38 percent of teens said young people do not respect each other's privacy online. Illegal downloads of software, music, and other intellectual property are widespread. The trends seem consistent across many countries. For example, a survey of Australian youth found 27 percent say they do things online that their parents would not approve of. In Spain, just 37 percent of teens say they would always ask a friend before posting that friend's photo online. In a U.S. study in 2008, 65 percent of teens said they illegally downloaded music in the past year.

- *Children need to learn basic citizenship on the Web--bullying, plagiarism and theft are just as wrong on the Internet as they are in the physical world. Children should have resources to deal with online bullying or harassment, and should understand the impact their postings or comments may have on others.*

### ***Education and Regulation, a Comparison***

Parents and teachers are best positioned to decide what content children should access online. Regulating children's Internet access may be appropriate in limited cases, including areas where age restrictions currently exist in the physical world—like gambling and pornography. But broader restrictions may actually undermine open communication between children and guardians about online activity. Better approaches, including education, open up the Internet and its tremendous opportunities to kids, while also providing safety guidelines. As United Nations Secretary-General Ban Ki-moon stated in May 2009, "The virtual world has exciting possibilities for nurturing children and helping them grow into creative, productive adults. But we must mind the pitfalls that could scar them for life."

### ***Funding: An Opportunity for Public-Private Partnership***

Mandatory education need not impose unfair burdens on teachers or school budgets. We recommend using federal funding sources, along with public-private partnerships, to support Internet safety education at the local level. State and local officials will often have valuable insights, as will teachers and librarians. Many employees of technology companies are prepared to serve as volunteers to introduce and implement online safety programs. In the United Kingdom and Australia, a program called "ThinkUKnow" pairs Microsoft employees with local law enforcement officials to deliver Internet safety education and resources to parents, teachers, and children.

High-quality curriculum materials are now available through these organizations:

i-SAFE [www.isafe.org/challels/?ch=ed](http://www.isafe.org/challels/?ch=ed)

WiredSafety [www.wiredsafety.org/educators.html](http://www.wiredsafety.org/educators.html)

Look Both Ways <http://www.ilookbothways.com/docs/DOC-1009>

NetSmartz [www.netsmartz.org/overview/statepartnerships.htm](http://www.netsmartz.org/overview/statepartnerships.htm).

You can find more information at the National Cyber Security Alliance website at <http://www.staysafeonline.info/>, and at Microsoft's Consumer online safety website: <http://www.microsoft.com/protect/default.mspx>.

*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT OR INFORMATION REFERENCED OR LINKED TO BY THIS DOCUMENT.*

© 2009 Microsoft Corporation. All rights reserved.