Children need to be active participants in becoming good digital citizens; they need to define their rights and responsibilities online, and have the skills to exercise their values and judgments to be as safe and secure as possible. Good ‘digizens’ can also be role models for others and inspire the online community in which they live.

Will Gardner, CEO, Childnet International, U.K.  
www.childnet-int.org

Good digital citizenship is key to everybody’s safety and success online, including children’s. At its core is learning how to be good to one another, which protects individuals and communities, increases social capital, and enables effective participation in today’s very social media environment. It brings relevance to online safety for youth because it demonstrates respect for their agency and the technologies they find so compelling and empowering. It turns users into stakeholders and agents for social good.

Anne Collier, Co-Director, ConnectSafely.org, U.S.  
www.connectsafely.org

By marrying the innovative approach of teaching 21st century skills with new notions of digital diplomacy, we can create 21st century citizens to inherit and inhabit our digital world. With the right combination of tools, rules and schools, we can inspire children to become good digital citizens by providing them with the skills they need to make smart choices online.


Our world is drastically different than the one in which our parents, or even we, grew up. Interpersonal relationships, the foundation of every society, are changing as technology has made it easier for people to engage with others located anywhere from their backyards to the Outback. Learning to be safe, ethical, healthy and resilient digital citizens is critical for youths’ success today and in the years to come.

Marsali Hancock, President and CEO, iKeepSafe, U.S.  
www.ikeepsafe.org

Teaching our children how to safely, ethically and productively use technology is a key component to ensuring a well-prepared workforce. What you do online and how you use technology has the potential to affect everyone—at home, at work and around the world. Practicing good online habits benefits the global, digital community. Microsoft has been a productive and positive partner with the NCSA by providing guidance and resources to empower a well-equipped digital citizenry.


Life online is what you make of it; just like in the real world there are simple steps you can take to ensure you have a safer Internet experience. It is important to ensure that the public is educated on Internet safety and that children know how to use the Internet and devices safely. Being an ethical and law-abiding digital citizen is essential to having safer and more secure interactions online.

Kevin Zuccato, Assistant Commissioner, Australian Federal Police, Australia

Our goal in the UAE is to foster a tech-savvy, self-aware youth. Microsoft is providing an excellent example of corporate social responsibility through its provision of resources worldwide to law enforcement services in the area of child awareness.

Lieutenant Colonel Faisal Al-Shamari, Member & Rapporteur of the United Arab Emirates Higher Child Protection Committee, Director of Child Protection Centre, Ministry of Interior
New information technologies have profoundly changed the world in which today’s young people learn and grow. The immense resources of the Internet and the accompanying array of Internet-enabled devices give young people tremendous opportunities to learn, share, and communicate. Today’s youth are immersed in this new digital environment. According to 2010 Pew research, 86 percent of European teens and 93 percent of U.S. teens are regularly online, and many young people are creating, actively contributing to, and engaging in their own digital culture.

According to a 2011 survey, 86 percent of U.S. parents stated that digital media is crucial to preparing young people for the twenty-first century. Yet adults also have concerns. The media, government, and law enforcement have given much attention to online safety issues including cyberbullying, child predators, sexting, pornography, digital plagiarism, violations of privacy, oversharing of personal information, Internet addiction, and pirated content.

Many countries have implemented a three-part approach to confront these issues—with technology tools, safety education, and law enforcement activities. All three play a vital role in protecting young people, but these strategies often consist of reactive responses to emerging safety concerns. A more advanced approach to online safety would include comprehensive measures, which take into account that young people must understand rules and behaviors that are unique to the digital world before they can become responsible citizens within emerging digital societies.
What is Digital Citizenship?

Digital citizenship is usually defined as “the norms of behavior with regard to technology use.” Mike Ribble, an education researcher and early advocate of digital citizenship, explains:

“Digital Citizenship is a concept which helps teachers, technology leaders and parents to understand what students/young people/technology users should know to use technology appropriately. Digital Citizenship is more than just a teaching tool; it is a way to prepare students/technology users for a society full of technology. Too often we are seeing students as well as adults misusing and abusing technology but not sure what to do. The issue is more than what the users do not know but what is considered appropriate technology usage.”
Why Digital Citizenship Matters

- Today’s young people are navigating a new digital culture in which the rules and social norms are sometimes unclear. They must learn about digital citizenship and develop a sense of ownership and personal responsibility to make good, ethical decisions in the online world.

- The online world presents great opportunities for young people, but it is not without risks. We can mitigate some of those risks by helping young people develop a strong sense of digital citizenship.

- Rather than relying solely on protective measures, an approach to online safety that includes digital citizenship will help young people safely interact in the online world. Teaching them about digital literacy and digital ethics and etiquette is no longer merely an option; it is an imperative.
Elements of Digital Citizenship

Digital Literacy
Digital citizenship means being digitally literate and having “the combination of skills, knowledge and understanding that young people need to learn before they can participate fully and safely in an increasingly digital world.” Many online safety incidents, such as inadvertent exposures of private information or security compromises through social engineering, are the result of a lack of digital literacy. Young people who are literate in the online world will have a better chance of avoiding risky situations, will make better decisions, and will better understand how to protect their privacy. But digital literacy involves more than just technical competency—it requires critical thinking skills in order to evaluate many different sources of information.

Digital Ethics & Etiquette
Although a technical knowledge of digital literacy provides a good foundation for digital citizenship, young people must learn digital ethics and etiquette before they can make the right decisions. Ethics will help young people make good ethical decisions, and etiquette will help them operate within online social norms. Many safety advocates believe that inappropriate online behavior such as bullying, plagiarism, and piracy are the direct result of poor ethics and a lack of etiquette.

93% OF U.S. AND 86% OF EUROPEAN TEENS ARE REGULARLY ONLINE AND CREATING THEIR OWN DIGITAL CULTURE.
In addition to the many online opportunities for young people, there are also potential problems that fall into three categories: content, conduct, and contact.
The Risks: Content

Inappropriate Content
Inappropriate content for young people includes sexually explicit websites, which are easily accessible online. Other content can be hateful, racist, or expressly violent. In 2009, 79 percent of U.S. young people, and 40 percent of European youth reported unwanted encounters with Internet pornography, and 49 percent reported viewing “hateful, sexist, or racist comments online.”

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

Stolen Content
Pirated software, music, movies, and other materials are widely available on the Internet. Because this material is so easily accessible, young people may not always appreciate the ethical implications of downloading, sharing or using pirated material. In fact, 86 percent of U.S. teens say they believe it is okay to illegally download and share music. Additionally, they may not realize the security risks associated with pirated content, which can contain malicious software.

86% of teens say they believe it’s okay to illegally download and share music

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

86% of teens say they believe it’s okay to illegally download and share music

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

86% of teens say they believe it’s okay to illegally download and share music

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

86% of teens say they believe it’s okay to illegally download and share music

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

86% of teens say they believe it’s okay to illegally download and share music

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

86% of teens say they believe it’s okay to illegally download and share music

Inaccurate Content
Inaccurate content, including biased, outdated, propagandistic, or misleading information, is an important concern, especially for young people who use the Internet for research or other educational purposes. Inexperienced young people may have trouble discerning which sources are credible and current, and they may not be able to distinguish legitimate research from propaganda. According to a study conducted in 2008, when U.S. high school students were asked to conduct health-related research, half of those asked produced inaccurate information gathered from the Internet.

86% of teens say they believe it’s okay to illegally download and share music
Addressing Youth and Content

Governments initially focused on legislative solutions for online content problems. In practice, though, many of these national laws proved marginally effective in restricting content, given the global nature of the Internet. Instead, online safety education coupled with technology tools such as content-filtering software are popular alternative solutions, which are used by 62 percent of U.S. parents\textsuperscript{15} and 85 percent of parents in the European Union (EU).\textsuperscript{16}

Although filtering and parental control technologies help reduce the risk of exposure to inappropriate material, technology alone cannot prepare young people for an unrestricted online world, which they will encounter by the time they are adults, if not sooner. Education that fosters digital citizenship goes beyond providing young people with a list of online safety rules and offers curriculum that engages young people and encourages their participation and decision-making.

Curriculum that is specifically designed to foster digital citizenship will help develop ethics in young people. A strong ethical foundation will help young people make better choices about online content, and it will help them more fully understand the implications of decisions about downloading and sharing pirated and plagiarized content. When young people learn critical thinking skills as they apply to online content, they will be better able to discern differences between good and bad or poor-quality material.
The Risks: Conduct

Cyberbullying

Cyberbullying has emerged as a major online safety issue. Surveys find that between 10 and 40 percent of young people in the European Union, the United States, South Korea, Japan, and Australia have been victims of cyberbullying. The U.S.-based Cyberbullying Research Center reports a link “between cyberbullying and low self-esteem, family problems, academic problems, school violence, and delinquent behavior.”

Inappropriate Sharing

Another conduct problem is the inappropriate sharing of personal information, which can be a form of bullying or a misguided attempt to attract attention. Although there is no evidence that posting generic personal information itself raises the risk to young people, there are clearly damaging consequences for transmitting some types of personal information. One of the most widely discussed forms of oversharing is the practice of transmitting sexually explicit photographs, commonly known as sexting. Pew Internet Research reports that 4 percent of 12- to-17-year-olds in the U.S. have sexted, while 15 percent have received sext messages.

Reputation

The consequences of oversharing can continue for years because content (such as inappropriate photos) can become part of a young person’s “digital dossier” available on the Internet. A 2010 survey from Microsoft found that, on average, more than 61 percent of Human Resources (HR) professionals in three countries reported reviewing online data when assessing potential job candidates. In the United States, 79 percent reported doing so, followed by Germany (59 percent) and the United Kingdom (47 percent).
Addressing Youth Issues with Conduct

As with content issues, initial responses to conduct problems like bullying have often involved proposed legislation, or the enforcement of existing legislation, such as laws against harassment. Although prosecuting clear cases of online harassment is uncontroversial, using child pornography laws to prosecute minors for sexting offenses has drawn criticism. In response, many localities are proposing or enacting new legislation to reduce penalties for sexting by minors.  

Online safety technologies are widely used to address content safety issues, but technology alone presents limited options for addressing issues of conduct. Parents can use filtering software, which blocks certain websites or webpages, but this method presents an all-or-nothing approach to restricting participation in online forums and social networks. Adults can also monitor young people’s behavior online with technology tools that record their activity, though some online safety experts express concern that this practice may undermine trust, and parents should disclose any monitoring to their children.

Protective measures, school discipline, and technology all play a role in addressing inappropriate conduct online. A more thoughtful approach, however, would include efforts to teach young people online ethics, help them develop empathy for others, and become “upstanders,” rather than bystanders, in response to online bullying and harassment.

79% 59% 47%

OF HR PROFESSIONALS REPORTED REVIEWING ONLINE INFORMATION WHEN EXAMINING POTENTIAL JOB CANDIDATES

U.S. GERMANY U.K.
The Risks: Contact

- No online safety issue has drawn as much attention or generated as much public concern as that of sexual predators’ contact with minors. A 2006 survey found that 4 percent of U.S. adolescents reported being sexually solicited online by an adult. Fewer actually fall victim to solicitations – about .03 percent, or 30 in 100,000 young people, reported physical sexual contact with an adult they met online.27
- Predators take advantage of the Internet’s anonymity to build online relationships with young people or to communicate with criminals who traffic young people for sex. Frequently, their goal is to develop what young people believe to be meaningful online relationships and later convince them to meet in person—a process referred to as online grooming.
- Unwanted contact can also include harassment, stalking, bullying, and other forms of victimization.

4% of U.S. adolescents report being sexually solicited online by an adult

Addressing Inappropriate Contact with Young People

Law enforcement efforts are central to the fight against the online exploitation of young people, and vigorous enforcement of such laws continues to have strong support. Customized web browsers can help restrict young people to approved Internet resources where they are unlikely to encounter adults. Other software can limit the use of communication technology to approved email or IM addresses. Monitoring tools that track online activity can help parents detect inappropriate contact, though some online safety experts express concern that this practice may undermine trust, and parents should disclose any monitoring to their children.

Most online safety programs already include warnings and safety tips for young people about avoiding unwanted contact from adults. Education that fosters digital citizenship builds on these warning systems, and encourages young people to make appropriate choices about social interaction, sharing, and producing content online. It also teaches the digital street smarts that young people need to avoid the Internet’s more unpleasant neighborhoods.
Taking Action

What Parents Can Do
- Talk to young people about appropriate online behavior and responsible use of technology
- Install parental controls such as filtering and monitoring software
- Establish rules and consequences for misbehavior online

What Educators Can Do
- Teach digital citizenship in primary and secondary schools so all young people can learn how to be responsible, respectful, and informed digital citizens
- Provide professional development to help teachers and staff with courses in digital citizenship

What the Technology Industry Can Do
- Create family-safety controls that allow parents to limit and monitor young people's online access
- Create and maintain conditions for online services that encourage civil behavior by deploying monitors that enforce policies against abusive behavior
- Create educational materials, and work with families and law enforcement agencies to promote digital citizenship
What Governments Can Do

The PointSmart.ClickSafe. Task Force contains several recommendations in its 2010 report:

- Expanding online safety efforts to emphasize online smarts, through digital media literacy and education programs that empower parents and teachers to prepare kids to navigate the world of online and digital media. These efforts will be significantly improved with more focus on education, rather than only on crime prevention.

- Consideration by education policymakers to adopt a set of national goals for online safety, including if possible minimum standards for a curriculum on digital literacy, to better educate young people and families about how to manage the media that daily infuse our lives.

- Ensure that all digital literacy and online safety programs are funded through competitive grants open to qualified applicants, with periodic review and assessment built into the grant process, so that the results from the best programs can be replicated in other communities.28

- Although there are many things that governments should do, it’s important to note what they should not do. While it is tempting to try to protect young people by passing technology mandates, the reality is that “tech mandates” have generally proven ineffective, given the global reach and scale of the Internet. Further, mandated technology may quickly become obsolete given the fast-paced and ever-changing nature of the digital world.

What Law Enforcement Can Do

- Create a safer environment by enforcing laws against harassment and sexual predators

- Support an advanced, effective online safety curriculum in schools, which is based on established research and accurately portrays risks

- Propose legislation that does not include excessive restrictions or mandates on technology
Digital Citizenship in a Connected World

An advanced approach to online safety—one centered on digital citizenship—offers more than fundamental protective measures; it combines the strengths of many strategies and resources to help prepare today's young people to be tomorrow's adults in an online, twenty-first century world. The online safety organization ConnectSafely summarizes the case for digital citizenship in its white paper Online Safety 3.0:

“When people see themselves as community stakeholders—citizens—they behave as citizens because they tend to care about the well-being of the community itself and the individual and collective behaviors that affect it. So what psychologists call ‘social norming’ happens—community members model good behaviors for each other, which is usually much more persuasive than rules or top-down efforts to control. Aggressive behavior is mitigated when young people receive training in citizenship, ethics, empathy, and new media literacy in the process of using social media and technologies as participants in a community of learners, and the results are empowerment as well as safety.”